Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

J.191

(03/2004)

SÉRIE J: RÉSEAUX CÂBLÉS ET TRANSMISSION DES SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET AUTRES SIGNAUX MULTIMÉDIAS

câblo-modems

Paquetage de fonctionnalités IP pour l'amélioration des câblo-modems

Recommandation UIT-T J.191

Recommandation UIT-T J.191

Paquetage de fonctionnalités IP pour l'amélioration des câblo-modems

Résumé

La présente Recommandation offre un ensemble de caractéristiques fondées sur le protocole IP qui peuvent être ajoutées à un câblo-modem ou être incorporées à un dispositif autonome afin de permettre aux câblo-opérateurs de fournir à leurs clients un ensemble supplémentaire de services améliorés comprenant la prise en charge de la qualité de service (QS) IPCablecom, une sécurité améliorée, des caractéristiques supplémentaires de gestion et d'approvisionnement, ainsi qu'un adressage et un traitement de paquets améliorés.

Source

La Recommandation UIT-T J.191 a été approuvée le 15 mars 2004 par la Commission d'études 9 (2001-2004) de l'UIT-T selon la procédure définie dans la Recommandation UIT-T A.8.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

TABLE DES MATIÈRES

		Page
1	Domaine d'application	1
2	Références	1
2.1	Références normatives	1
2.2	Références informatives	4
3	Termes et définitions	4
4	Abréviations, acronymes et conventions	5
4.1	Abréviations et acronymes	5
4.2	Conventions	7
5	Architecture de référence	8
5.1	Architecture de référence logique	9
5.2	Modèle de référence fonctionnel IPCable2Home	12
5.3	Modèle d'interface de messagerie IPCable2Home	16
5.4	Modèle de référence d'information IPCable2Home	17
5.5	Modèles fonctionnels IPCable2Home	20
5.6	Interfaces physiques IPCable2Home	22
6	Utilitaires de gestion	23
6.1	Introduction/Aperçu général	23
6.2	Architecture de gestion	24
6.3	Le portail de gestion du câble (CMP)	25
6.4	Le portail d'essai du câble (CTP, *cable test portal*)	49
6.5	Rapport d'événement	54
7	Utilitaires d'approvisionnement	60
7.1	Introduction/aperçu général	60
7.2	Architecture de portail DHCP du câble	63
7.3	Architecture de configuration globale des services PS	85
7.4	Architecture du client d'heure actuelle	98
8	Traitement de paquet et traduction d'adresse	101
8.1	Introduction/Aperçu général	101
8.2	Architecture	101
8.3	Exigences relatives au portail CAP	109
9	Résolution de nom	112
9.1	Introduction/Aperçu général	112
9.2	Architecture	113
9.3	Exigences relatives à la résolution des noms	115
10	Qualité de service	116
10.1	Introduction	116
10.2	Architecture de qualité de service	117

10.3 Exigences relatives à la messagerie de qualité de service du câble 119
11 Sécurité 119
11.1 Introduction/Aperçu général 119
11.2 Architecture de sécurité 120
11.3 Exigences 125
12 Processus de gestion 173
12.1 Introduction/Aperçu général 173
12.2 Processus d'utilitaires de gestion 173
12.3 Fonctionnement du service portail 176
12.4 Accès de base MIB 179
13 Processus d'approvisionnement 184
13.1 Modes d'approvisionnement 186
13.2 Processus d'approvisionnement du service portail pour la gestion en mode d'approvisionnement DHCP 188
13.3 Processus d'approvisionnement du service portail pour la gestion en mode d'approvisionnement SNMP 195
13.4 Processus d'approvisionnement PS/WAN-Data 203
13.5 Processus d'approvisionnement: client DHCP dans le secteur LAN-Trans 205
13.6 Processus d'approvisionnement: client DHCP dans le secteur LAN-Pass 207
Annexe A – Objets de base MIB 209
Annexe B – Format et contenu des événements, de l'enregistrement SYSLOG et des transferts TRAP du protocole SNMP 221
B.1 Description des transferts automatiques 231
Annexe C – Dangers et mesures préventives 231
C.1 Dangers 231
C.2 Mesures préventives 232
Annexe D – Applications de traduction CAT et de pare-feu 233
Annexe E – Bases MIB 234
E.1 Base MIB de service portail (PS) 234
E.2 Base MIB de portail d'essai du câble 245
E.3 Base MIB de sécurité 253
E.4 Définition 258
E.5 Base MIB de portail DHCP du câble (CDP) 259
E.6 Portail d'adresse câble (CAP) 272

Recommandation UIT-T J.191

Paquetage de fonctionnalités IP pour l'amélioration des câblo-modems

1 Domaine d'application

La présente Recommandation offre un ensemble de caractéristiques fondées sur le protocole IP qui peuvent être ajoutées à un câblo-modem ou être incorporées dans un dispositif autonome afin de permettre aux câblo-opérateurs de fournir à leurs clients un ensemble supplémentaire de services améliorés comprenant la prise en charge de la qualité de service (QS) IPCablecom, une sécurité améliorée, des caractéristiques supplémentaires de gestion et d'approvisionnement, ainsi qu'un adressage et un traitement de paquets améliorés. La présente Recommandation implémente le domaine IPCable2Home qui est défini dans la Rec. UIT-T J.190.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

2.1 Références normatives

– Recommandation UIT-T J.112 Annexe B (2004), *Spécifications de l'interface du service de transmission de données par câble: interface radioélectrique*.

– Recommandation UIT-T J.161 (2001), *Caractéristiques des codecs audio destinés au service audio bidirectionnel sur les réseaux de télévision par câble utilisant des câblo-modems*.

– Recommandation UIT-T J.163 (2004), *Qualité de service dynamique pour la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems*.

– Recommandation UIT-T J.170 (2002), *Spécification de la sécurité sur IPCablecom*.

– Recommandation UIT-T X.509 (2000) | ISO/CEI 9594-8:2001, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

– Recommandation UIT-T X.690 (2002) | ISO/CEI 8825-1:2002, *Technologies de l'information – Règles de codage ASN.1: spécification des règles de codage de base, des règles de codage canoniques et des règles de codage distinctives*.

– ISO/CEI 15802-3:1998 (ANSI/IEEE Std 802.1D), *Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseaux locaux et métropolitains – Spécifications communes – Partie 3: Ponts du contrôle d'accès au support*.

– FIPS 140-2-2001, *Security Requirements for Cryptographic Modules (Règles de sécurité pour modules cryptographiques)*.

– FIPS 180-2-2002, *Secure hash standard (Algorithme de hachage sécurisé)*.

– FIPS 186-2-2000, *Digital signature standard (DSS) (Norme de signature numérique)*.

– IETF RFC 768 (1980), *User Datagram Protocol (UDP) (Protocole des datagrammes d'utilisateur)*.

– IETF RFC 792 (1981), *Internet Control Message Protocol, DARPA Internet Program, Protocol specification (Protocole des messages de commande de l'Internet)*.

– IETF RFC 868 (1983), *Time Protocol (Protocole temporel)*.

– IETF RFC 1034 (1987), *Domain Names – Concepts and Facilities (Noms de domaines – Concepts et services).*

– IETF RFC 1035 (1987), *Domain Names – Implementation and Specification (Noms de domaines – Mise en œuvre et spécification)*.

– IETF RFC 1122 (1989), *Requirements for Internet Hosts – Communication layers (Exigences pour les serveurs Internet – Couches de communication).*

– IETF RFC 1157 (1990), *A Simple Network Management Protocol (SNMP) (Un protocole simple de gestion de réseau)*.

– IETF RFC 1350 (1992), *The TFTP Protocol (Revision 2) (Le protocole TFTP)*.

– IETF RFC 1901 (1996), *Introduction to community-based SNMPv2 (Introduction à la version 2 du protocole SNMP de communauté)*.

– IETF RFC 2011 (1996), *SNMPv2 Management Information Base for the Internet Protocol using SMIv2 (Base d'informations de gestion SNMPv2 pour le protocole Internet utilisant la version SMIv2)***.**

– IETF RFC 2013 (1996), *SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2 (Base d'informations de gestion SNMPv2 pour le protocole de datagrammes d'utilisateur utilisant la version SMIv2)*.

– IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol (Protocole de configuration dynamique de serveur)*.

– IETF RFC 2132 (1997), *DHCP Options and BOOTP Vendor Extensions (Options DHCP et extensions BOOTP de vendeur)*.

– IETF RFC 2233 (1997), *The Interfaces Group MIB using SMIv2 (La base MIB de groupe d'interfaces utilisant la version SMIv2)*.

– IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2 (Protocole de gestion de groupe Internet, Version 2)*.

– IETF RFC 2315 (1998), *PKCS #7: Cryptographic Message Syntax Version 1.5 (Système PKCS n° 7: Syntaxe de message cryptographique, Version 1.5)*.

– IETF RFC 2437 (1998), *PKCS #1: RSA Cryptography Specifications Version 2.0 (Système PKCS n° 1: Spécifications de cryptographie par algorithme RSA, Version 2.0)*.

– IETF RFC 2576 (2000), *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework (Coexistence entre les versions 1, 2 et 3 du cadre de gestion de réseau par la norme Internet)*.

– IETF RFC 2578 (1999), *Structure of Management Information Version 2 (SMIv2) (Structure de la version 2 des informations de gestion (SMIv2))*.

– IETF RFC 2579 (1999), *Textual Conventions for SMIv2 (Conventions textuelles pour la version SMIv2)*.

– IETF RFC 2580 (1999), *Conformance Statements for SMIv2 (Déclarations de conformité pour la version SMIv2)*.

– IETF RFC 2669 (1999), *DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems (Base MIB de dispositifs par câble DOCSIS – Base d'informations de gestion de dispositif par câble pour câblo-modems et systèmes de terminaison de câblo-modem conformes à DOCSIS)*.

– IETF RFC 2670 (1999), *Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS compliant RF interfaces (Base d'informations de gestion d'interface radioélectrique pour interfaces RF conformes aux systèmes MCNS/DOCSIS)*.

– IETF RFC 2786 (2000), *Diffie-Helman USM Key Management Information Base and Textual Convention (Base d'informations de gestion de clés dans le modèle USM à codage Diffie-Helman et convention textuelle)*.

– IETF RFC 2863 (2000), *The Interfaces Group MIB (Base d'information de gestion de groupe d'interfaces)*.

– IETF RFC 3022 (2001), *Traditional IP Network Address Translator (Traditional NAT) (Convertisseur d'adresse de couche réseau IP traditionnel (conversion NAT traditionnelle))*.

– IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (Certificat et profil de liste CRL d'infrastructure de clé publique Internet X.509)*.

– IETF RFC 3291 (2002), *Textual Conventions for Internet Network Addresses (Conventions textuelles pour adresses de réseau Internet)*.

– IETF RFC 3396 (2002), *Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4) (Codage d'options longues dans le protocole de configuration dynamique de serveur) (DHCPv4)*.

– IETF RFC 3412 (2002), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) (Traitement et distribution de messages pour le protocole simple de gestion de réseau) (SNMP)*.

– IETF RFC 3413 (2002), *Simple Network Management Protocol (SNMP) applications (Applications du protocole SNMP)*.

– IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) (Modèle de sécurité du point de vue de l'utilisateur pour la version 3 du protocole simple de gestion de réseau)*.

– IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) (Modèle de contrôle d'accès fondé sur la vue pour le protocole simple de gestion de réseau)*.

– IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for Simple Network Management Protocol (SNMP) (Version 2 des opérations protocolaires du protocole simple de gestion de réseau) (SNMP)*.

– IETF RFC 3417 (2002), *Transport Mappings for the Simple Network Management Protocol (SNMP) (Mappages de transport pour le protocole simple de gestion de réseau) (SNMP)*.

– IETF RFC 3418 (2002), *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) (Base d'informations de gestion (MIB) pour le protocole simple de gestion de réseau (SNMP)*.

2.2 Références informatives

– Recommandation UIT-T J.190 (2002), *Architecture de MediaHomeNet prenant en charge les services câblés*.

– IETF RFC 347 (1972), *Echo Process (Traitement de l'écho)*.

– IETF RFC 1949 (1996), *Scalable Multicast Key Distribution (Distribution de clés modulable en multidiffusion)*.

– IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations (Terminologie et considérations relatives au convertisseur d'adresses IP de réseau (NAT))*.

– IETF RFC 2979 (2000), *Behavior of and Requirements for Internet Firewalls (Comportement et prescriptions des pare-feu Internet)*.

– IETF RFC 3235 (2002), *Network Address Translator (NAT) – Friendly Application Design Guidelines (Convertisseur d'adresses de réseau – Directives de conception d'applications conviviales)*.

– draft-ietf-ipcdn-bpiplus-mib-12 INTERNET DRAFT – *DOCSIS Baseline Privacy Plus MIB – Management Information Base for DOCSIS Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus (Projet Internet – Base d'informations de gestion pour la confidentialité de base améliorée DOCSIS – Base d'informations de gestion pour les câblo-modems DOCSIS et les systèmes de terminaison de câblo-modems pour la confidentialité de base améliorée) octobre 2003*.

– ICSA, Inc.: Firewall Buyer's Guide, 1998, *www.icsalabs.com (Guide de l'acheteur de pare-feu)* http://www.icsalabs.com.

3 Termes et définitions

La présente Recommandation définit les termes suivants:

3.1 portail de sécurité de câble (CSP, *cable security portal*): élément fonctionnel qui fournit des fonctions de gestion de la sécurité et de conversion entre l'hybride HFC et l'utilisateur résidentiel.

3.2 serveur de gestion d'appel (CMS, *call management server*) [IPCablecom]: serveur qui contrôle les connexions audio, également appelé *agent d'appel* dans la terminologie du protocole MGCP/SGCP.

3.3 qualité de service dynamique (DQoS, *dynamic quality of service*) [IPCablecom]: qualité attribuée au fur et à mesure à chaque communication selon la qualité de service requise.

3.4 adaptateur de terminal multimédia imbriqué (E-MTA, *embedded multimedia terminal adapter*) [IPCablecom]: nœud simple qui contient à la fois un adaptateur MTA et un câblo-modem.

3.5 câblo-modem IP amélioré: câblo-modem qui a été amélioré par l'ajout des dispositifs IP de la présente Recommandation.

3.6 service portail (PS, *portal service*): élément fonctionnel qui fournit des fonctions de gestion et de traduction entre l'hybride HFC et l'utilisateur résidentiel.

3.7 dispositif IP de réseau local: dispositif IP typique qui est censé résider chez l'utilisateur résidentiel et qui contient une pile de protocoles TCP/IP ainsi qu'un client du protocole DHCP.

3.8 traversée: sous-fonction du portail CAP qui transfère sans changement les paquets du côté WAN-Data au côté LAN-Pass du portail CAP.

3.9 adaptateur de terminal multimédia autonome (S-MTA, *stand-alone multimedia terminal adapter*): nœud unique qui contient un adaptateur MTA et une commande MAC non DOCSIS (par exemple, Ethernet).

4 Abréviations, acronymes et conventions

4.1 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ASP	mandataire spécifique de l'application (*application-specific proxy*)
CA	autorité de certification (*certificate authority*)
CAP	portail d'adresse câble (*cable address portal*)
CAT	traduction d'adresse câble (*cable address translation*)
CDC	client de protocole DHCP de câble (*cable DHCP Client*)
CDP	portail de protocole DHCP de câble (*cable DHCP portal*)
CDS	serveur de protocole DHCP du câble (*cable DHCP server*)
CM	câblo-modem
CMP	portail de gestion du câble (*cable management portal*)
CMS	serveur de gestion d'appels (*call management server*)
CMTS	système de terminaison de câblo-modem (*cable modem termination system*)
C-NAPT	traduction d'adresse et portail réseau câblé (*cable network address and portal translation*)
C-NAT	traduction d'adresse de réseau câblé (*cable network address translation*)
CNP	portail de nommage du câble (*cable naming portal*)
CQoS	qualité de service du câble (*cable quality of service*)
CQP	portail de qualité de service du câble (*cable quality of service portal*)
CRL	liste de révocation de certificat (*certificate revocation list*)
CSP	portail de sécurité de câble (*cable security portal*)
CTP	portail d'essai du câble (*cable testing portal*)
CVC	certificat de vérification de code
CVS	signature de vérification de code (*code verification signature*)
CxP	sous-fonction du service portail sur le câble (*cable PS sub-function*)
DER	règles de codage distinctives (*distinguished encoding rules*)
DHCP	protocole de configuration de serveur dynamique (*dynamic host configuration protocol*)
DNS	système de dénomination de domaine (*domain name system*)
DOCSIS	spécification d'interface du service de transmission de données par câble (*data-over-cable service interface specification*)
DQoS	qualité de service dynamique (IPCablecom) (*dynamic quality of service (IPCablecom)*)

E-MTA	adaptateur de terminal multimédia imbriqué (*embedded multimedia terminal adapter*)
FTP	protocole de transfert de fichiers (*file transfer protocol*)
FW	pare-feu (*firewall*)
GMT	temps moyen de Greenwich (*Greenwich mean time*)
HEX	hexadécimal
HFC	hybride optique coaxial (*hybrid fibre coax*)
ICMP	protocole des messages de commande Internet (*Internet control message protocol*)
IGMP	protocole de gestion de groupe Internet (*Internet group management protocol*)
IP	protocole Internet (*Internet protocol*)
KDC	centre de distribution de clé (*key distribution centre*)
LAN-Pass	adresse LAN de traverse (*pass-through LAN address*)
LAN-Trans	adresse LAN traduite (*translated LAN address*)
MAC	commande d'accès au support (*media access control*)
MGCP	protocole de contrôle de passerelle média (*media gateway control protocol*)
MIB	base d'informations de gestion (*management information base*)
MTA	adaptateur de terminal multimédia (*multimedia terminal adapter*)
NAPT	traduction d'adresse et portail réseau (*network address and portal translation*)
NAT	traduction d'adresse de réseau (*network address translation*)
NCS	signalisation d'appel fondée sur le réseau (*network-based call signalling*)
NMS	système de gestion de réseau (*network management system*)
OID	identificateur d'objet (*object identifier*)
OSI	interconnexion des systèmes ouverts (*open systems interconnection*)
OSS	système support d'exploitation (*operations support system*)
PDU	unité de données protocolaire (*protocol data unit*)
PING	groupeur interréseau de paquets (*packet inter-network grouper*)
PKI	infrastructure de clé publique (*public key infrastructure*)
PKINIT	authentification initiale par cryptographie à clé publique (*public-key cryptography for initial authentication*)
PS	service portail (*portal service)*
PS WAN-Data	interface de données de réseau WAN d'élément de service portail (*portal service element WAN data interface*)
PS WAN-Man	interface de gestion de réseau WAN d'élément de service portail (*portal service element WAN management interface*)
QS	qualité de service
RFC	demande de commentaires (*request for comments*)
RSA	Rivest, Shamir, Adleman
SHA-1	algorithme de hachage sécurisé n° 1 (*secure hash algorithm 1*)

S-MTA adaptateur autonome de terminal multimédia (*stand-alone multimedia terminal adapter*)

SNMP protocole simple de gestion de réseau (*simple network management protocol*)

SOA début d'autorité (*start of authority*)

SPF filtrage de paquet d'après l'état (*stateful packet filtering*)

SYSLOG enregistrement système (*system log*)

TCP protocole de commande de transmission (*transmission control protocol*)

TFTP protocole trivial de transfert de fichiers (*trivial file transfer protocol*)

TLV type-longueur-valeur

UDP protocole datagramme d'utilisateur (*user datagram protocol*)

USFS commutation de transmission sélective de sens montant (*upstream selective forwarding switch*)

USM modèle de sécurité d'utilisateur (*user security model*)

UTC temps universel coordonné (*coordinated universal time*)

VACM modèle de commande d'accès fondé sur la vue (*view-based access control model*)

VoIP téléphonie utilisant le protocole Internet (*voice over Internet protocol*)

WAN réseau régional (*wide area network*)

WAN-Data secteur d'adresse de données de réseau régional (*wide area network data address realm*)

WAN-Man secteur d'adresse de gestion de réseau régional (*wide area network management address realm*)

4.2 Conventions

Pour l'implémentation de la présente Recommandation, les mots clés "DOIT" et "REQUIS" sont à interpréter comme indiquant un aspect obligatoire de la présente Recommandation. Les mots clés indiquant un certain niveau de portée d'exigences particulières, qui sont utilisés tout au long de la présente Recommandation, sont résumés ci-dessous.

"DOIT" Cette forme verbale ou l'adjectif "REQUIS" signifie que le sujet est une exigence absolue de la présente Recommandation.

"NE DOIT PAS" Cette expression signifie que le sujet est une interdiction absolue de la présente Recommandation.

"DEVRAIT" Cette forme verbale ou l'adjectif "RECOMMANDÉ" signifie qu'il peut exister, dans des circonstances particulières, des raisons valides pour ignorer ce sujet; mais il faut en comprendre toutes les implications et peser attentivement le cas avant de choisir une option différente.

"NE DEVRAIT PAS" Cette expression signifie qu'il peut exister, dans des circonstances particulières, des raisons valides pour que le comportement indiqué soit acceptable ou même utile; mais il faut en comprendre toutes les implications et peser attentivement le cas avant d'implémenter un quelconque comportement décrit avec cette mention.

"PEUT" Cette forme verbale ou l'adjectif "FACULTATIF" signifie que le sujet est véritablement facultatif. Un vendeur peut choisir d'inclure le sujet parce qu'un marché particulier le requiert ou, par exemple, parce que le sujet améliore le produit; un autre vendeur peut omettre le même sujet.

5 Architecture de référence

La présente Recommandation offre un ensemble de caractéristiques fondées sur le protocole IP qui peuvent être ajoutées à un câblo-modem ou être implémentées dans un dispositif autonome afin de permettre aux câblo-opérateurs de fournir à leurs clients un ensemble supplémentaire de services améliorés. Ces caractéristiques fondées sur le protocole IP résident dans un élément logique appelé *service portail* (*PS* ou simplement *portail*). Un dispositif contenant ces caractéristiques améliorées est désigné sous le nom de *passerelle résidentielle*, qui est une implémentation du système IPCable2Home tel que décrit dans la Rec. UIT-T J.190.

Les principaux domaines et les principales caractéristiques sont énumérés ci-dessous:

– gestion et approvisionnement:
  - gestion à distance et configuration de la passerelle résidentielle;
  - mandataire de gestion simple de passerelle résidentielle pour les dispositifs résidentiels en protocole IP;
  - approvisionnement automatique pour les dispositifs de passerelle résidentielle;
– adressage et traitement de paquet:
  - conversion d'une adresse en plusieurs pour les dispositifs résidentiels;
  - conversion d'adresse une à une pour les dispositifs résidentiels;
  - adressage sans conversion pour dispositifs résidentiels (à applications allergiques à la conversion NAT);
  - protection du trafic par hybride HFC vis-à-vis des communications internes par dispositif résidentiel;
  - prise en charge de l'adressage résidentiel au cours d'un délestage d'hybride HFC;
  - serveur DNS simple dans la passerelle résidentielle;
– qualité de service (QS):
  - fonction de dérivation transparente dans le dispositif de passerelle résidentielle pour les messages de qualité de service IPCablecom au départ/à destination d'applications compatibles avec le système IPCablecom;
– sécurité:
  - authentification du dispositif de passerelle résidentielle;
  - messages de gestion sécurisés dans la passerelle résidentielle;
  - téléchargement sécurisé de fichiers de configuration et de mise à jour logicielle;
  - qualité de service sécurisée sur la liaison par hybride HFC;
  - gestion à distance de pare-feu de passerelle résidentielle.

La communication dans les réseaux WAN et LAN est en protocole IPv4, par déploiement des protocoles spécifiquement définis dans le reste de la présente Recommandation. Les dispositifs conformes DOIVENT implémenter la version 4 de la suite des protocoles IP (IPv4).

Le reste du présent paragraphe considère l'architecture de référence logique à partir des six points de vue suivants:

- point de vue logique (§ 5.1);
- point de vue fonctionnel (§ 5.2);
- point de vue de l'interface de messagerie (§ 5.3);
- point de vue informationnel (§ 5.4);
- point de vue opérationnel (§ 5.5);
- point de vue de l'interface physique (§ 5.6).

5.1 Architecture de référence logique

Comme indiqué dans la Figure 5-1, le présent paragraphe introduit les concepts logiques du domaine IPCable2Home, les éléments logiques et la classe des dispositifs d'accès résidentiel (HA, *home access*).

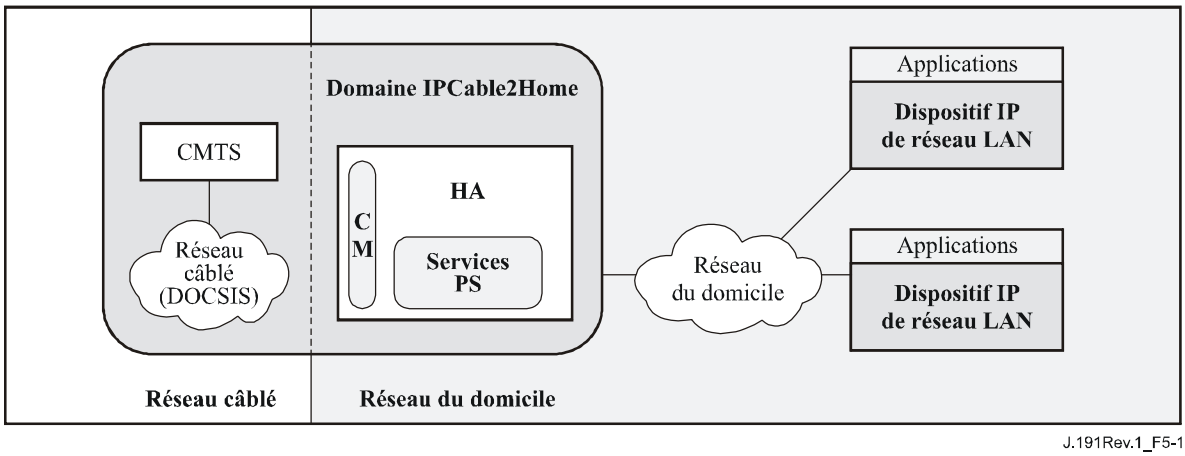


Figure 5-1/J.191 – Principaux concepts logiques

5.1.1 Domaines IPCable2Home

Le domaine IPCable2Home représente l'ensemble des éléments de réseau qui sont conformes à la présente Recommandation. Ce domaine est représenté sous forme schématique par la zone ombrée de la Figure 5-1. Cette région sert d'utilitaire visuel permettant de repérer clairement les éléments du réseau du domicile qui sont conformes. Les éléments qui résident à l'intérieur du domaine IPCable2Home (c'est-à-dire les éléments conformes) sont directement gérables par les opérateurs.

5.1.2 Eléments logiques

Le cadre architectural introduit le concept d'éléments logiques IPCable2Home. Ces derniers sont des entités fonctionnelles associées logiquement qui peuvent produire des messages conformes à IPCable2Home et qui peuvent y répondre. Les éléments logiques IPCable2Home fonctionnent dans la couche du protocole de réseau et dans les couches supérieures, ce qui leur permet de rester indépendants de toute technique particulière de réseau physique. Ces éléments possèdent également la capacité de recueillir et de communiquer, selon les besoins, des informations permettant de gérer et d'acheminer des services dans les réseaux IPCable2Home. La présente Recommandation définit une seule entité logique, qui est désignée comme étant l'élément de services PS (PS, *portal service*).

5.1.2.1 Services PS (PS)

Un portail est un élément logique qui fournit dans les bâtiments des services composites de sécurité, de gestion, d'approvisionnement et d'adressage. Trois ensembles de fonctions de services portail sont définis: l'ensemble des fonctions de gestion, l'ensemble des fonctions de qualité de service (QS) et l'ensemble des fonctions de sécurité. L'élément logique de services portail constitue la base de l'architecture de référence logique.

5.1.3 Classes de dispositifs

Le cadre architectural fait également appel au concept de classes de dispositifs afin de fournir un contexte tangible aux éléments logiques et à leurs diverses combinaisons. Le concept IPCable2Home de classe de dispositif n'impose aucune restriction aux dispositifs physiques ou aux combinaisons d'éléments logiques situées à l'intérieur de dispositifs physiques. Les classes de dispositifs permettent d'offrir une information descriptive d'ensembles d'éléments logiques mais ne sont pas considérées comme étant définitives ou restrictives.

Dans le système IPCable2Home, la classe des dispositifs d'accès résidentiel (HA) représente l'emplacement physique de l'élément logique PS et permet aux éléments de réseau contenus dans le domaine IPCable2Home d'interagir avec les dispositifs IP d'un réseau LAN. Le dispositif d'accès résidentiel (HA) possède une seule interface radioélectrique conforme avec un câblo-modem, possède un seul élément logique PS et peut avoir zéro, une ou plusieurs interface(s) IP avec des réseaux LAN.

La présente Recommandation fait également référence à des dispositifs IP de réseau LAN qui représentent des dispositifs IP typiquement censés résider dans des réseaux résidentiels et censés contenir une pile TCP/IP ainsi qu'un client de protocole DHCP.

5.1.3.1 Eléments PS imbriqués ou autonomes

Les deux composants primaires qui peuvent être intégrés dans une passerelle résidentielle – à savoir le câblo-modem (CM) conforme à la norme DOCSIS et l'élément de services portail (PS) – peuvent utiliser des ressources matérielles et logicielles communes ou indépendantes. C'est ce partage de ressources entre CM et PS qui distingue le service PS autonome du service PS imbriqué.

Un service PS autonome NE DOIT PAS partager de composants matériels ou logiciels avec un CM. La séparation du CM vis-à-vis des services PS autonomes DOIT apparaître au service PS comme une simple déconnexion de son réseau WAN, c'est-à-dire que le service portail (PS) restera entièrement fonctionnel, comme s'il avait été déconnecté du réseau WAN. Sinon, le service PS sera considéré comme étant imbriqué. Compte tenu de ces définitions, il est possible qu'un PS puisse résider à l'intérieur de la même enceinte physique qu'un CM tout en restant considéré comme un service PS autonome.

CM et PS sont considérés comme des éléments distincts, aussi bien dans le cas de l'autonomie que dans celui de l'imbrication. Ils répondent à des adresses de gestion uniques. Dans le cas de l'imbrication, CM et PS peuvent se partager des composants matériels ou logiciels mais, du point de vue de la gestion, ce sont des entités distinctes.

La Figure 5-2 décrit les deux services PS, autonome et imbriqué. Dans les deux cas, la combinaison d'un CM et d'un PS est considérée comme intégrant le concept du dispositif d'accès résidentiel (HA). En d'autres termes, un dispositif HA se compose d'un unique CM et d'un unique PS. Cette hypothèse d'association d'un seul PS par CM reste vraie même si le service PS est autonome, c'est-à-dire que l'on suppose qu'un seul service portail autonome peut se connecter à un câblo-modem donné.

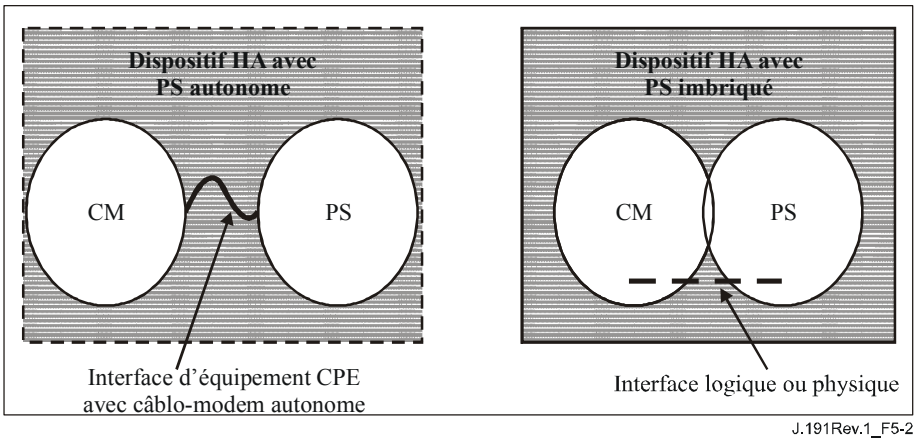


Figure 5-2/J.191 – Service PS autonome et service PS imbriqué

5.1.4 Secteurs d'adresses

Un secteur d'adresses se définit comme "un domaine de réseau dans lequel les adresses de couche Réseau sont attribuées de façon univoque aux entités de telle sorte que les datagrammes puissent leur être acheminés" [RFC 2663]. Dans la présente Recommandation, les secteurs d'adresses entrent dans les deux catégories suivantes: WAN et LAN (voir Figure 5-3).

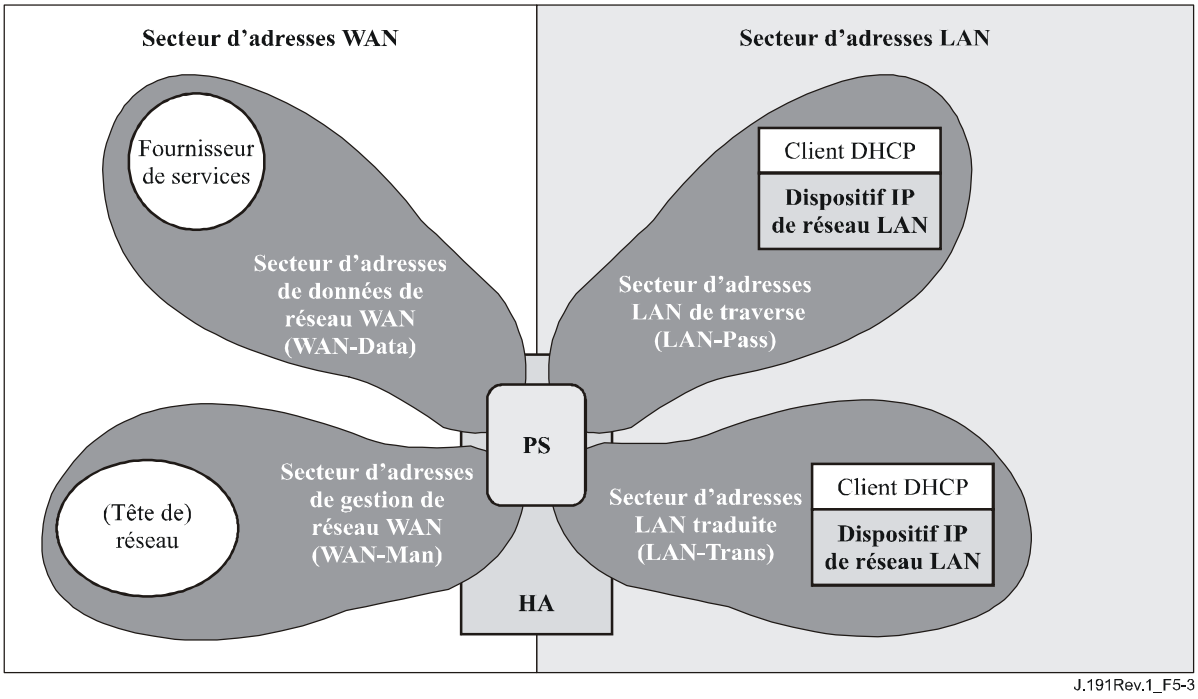


Figure 5-3/J.191 – Secteurs d'adresses

Les adresses de réseau WAN résident dans un des deux secteurs suivants: le secteur d'adresse de gestion de réseau régional (WAN-Man, *wide area network management address realm*) ou le secteur d'adresse de données de réseau régional (WAN-Data, *wide area network data address realm*). Les adresses de réseau LAN résident aussi dans l'un des deux secteurs suivants: secteur d'adresse LAN de traverse (LAN-Pass, *pass-through LAN address*) ou secteur d'adresse LAN traduite (LAN-Trans, *translated LAN address*). Les propriétés de ces secteurs d'adressage sont décrites ci-dessous:

- le secteur d'adresse de gestion de réseau WAN (WAN-Man) est destiné à transporter du trafic de gestion de réseau sur le réseau câblé entre le système de gestion du réseau et l'élément de services PS. En principe, les adresses de ce secteur résident dans l'espace privé d'adresse IP;
- le secteur d'adresse de données de réseau WAN (WAN-Data) est destiné à transporter du trafic d'application d'abonné sur le réseau câblé et au-delà, comme le trafic entre dispositifs IP de réseau LAN et serveurs Internet. En principe, les adresses de ce secteur résident dans l'espace public d'adresse IP;
- le secteur d'adresse LAN traduite (LAN-Trans) est destiné à transporter du trafic d'application d'abonné et du trafic de gestion sur le réseau interne entre les dispositifs IP du réseau LAN et le service portail. En principe, les adresses de ce secteur résident dans l'espace privé d'adresse IP et peuvent en principe être réutilisées par les abonnés;
- le secteur d'adresse LAN de traverse (LAN-Pass) est destiné à transporter du trafic d'application d'abonné, par exemple du trafic entre dispositifs IP de réseau LAN et serveurs Internet, sur la liaison interne, sur le réseau câblé, et au-delà. En principe, les adresses de ce secteur résident dans l'espace public d'adresse IP.

Du côté du réseau LAN, les adresses contenues dans le secteur d'adresse LAN de traverse (LAN-Pass) sont directement extraites des adresses contenues dans le secteur d'adresse de réseau WAN-Data. Celles-ci sont utilisées par les dispositifs IP de réseau LAN et par des applications telles que les services IPCablecom qui n'acceptent pas la conversion d'adresse et exigent une adresse IP acheminable mondialement. De plus, du côté LAN, les dispositifs IP de réseau LAN peuvent utiliser des adresses traduites venant du secteur d'adresses LAN traduites (LAN-Trans).

Les interfaces physiques avec le réseau LAN qui sont contenues dans le service portail se font attribuer un indice conformément à la base MIB de groupe d'interfaces [RFC 2233] comme décrit dans le § 6.3.8. Une interface virtuelle avec le réseau LAN, intégrant les interfaces physiques avec le réseau LAN, est également définie pour le service portail dans le § 6.3.8. L'adresse IP du côté LAN qui a été définie pour le service PS est "reliée" à cette interface virtuelle. Les fonctions de protocole DHCP et de serveur de noms de domaine du service PS, ainsi que la fonction de routeur du service PS, sont des applications implémentées dans le service PS adressé au moyen de l'adresse IP du côté LAN qui est reliée à l'interface virtuelle avec le réseau LAN.

5.2 Modèle de référence fonctionnel IPCable2Home

Les fonctions IPCable2Home sont des services (de couche 3 et de couches supérieures) qui ont été définis pour le système IPCable2Home. Ces fonctions sont implantées dans le service portail (PS), dans les dispositifs IP de réseau LAN et dans la tête de réseau. Il existe des fonctions IPCable2Home pour chacun des principaux domaines de spécification: approvisionnement et gestion, sécurité et qualité de service: ces fonctions sont brièvement décrites dans les trois paragraphes qui suivent.

5.2.1 Fonctions de gestion

Trois classes de fonctions de gestion sont définies pour la prise en charge de l'approvisionnement et de la gestion des dispositifs IP de réseau LAN:

- fonctions de serveur de gestion;

- fonctions de client de gestion;
- fonctions de portail de gestion.

Plusieurs des fonctions de serveur de gestion résident au sein de la tête de réseau (HE, *headend*). Les fonctions de client de gestion se trouvent en principe au sein des dispositifs IP de réseau LAN. Les fonctions de portail de gestion se situent au sein de l'élément logique de services portail et peuvent inclure des fonctionnalités d'émulation de serveur, de client et de relais afin d'agréger et de convertir les messages entre la tête de réseau et les dispositifs IP de réseau LAN. Des exemples de fonctions de serveur de gestion, de services portail et de client sont introduites dans les Tableaux 5-1, 5-2 et 5-3. Ces exemples sont également décrits par la Figure 5-4.

Tableau 5-1/J.191 – Description de la fonction de serveur de gestion

Fonctions de serveur de gestion	Description
Serveur DHCP de tête de réseau	Composant de tête de réseau qui fournit au service portail les informations d'adresse pour les secteurs d'adresses WAN-Man et WAN-Data.
Serveur de messagerie de gestion de tête de réseau	Serveurs de messagerie de gestion, de téléchargement et de notification d'événement de la tête de réseau, y compris les protocoles tels que SNMP, SYSLOG et TFTP.

Tableau 5-2/J.191 – Description de la fonction de portail de gestion et d'approvisionnement

Fonctions de portail de gestion	Description
Portail d'adresse câble (CAP, *cable address portal*)	Au sein des services PS, le portail CAP interconnecte les secteurs d'adresses WAN et LAN pour le trafic de données. (Voir CAT/traversée).
Traduction d'adresse câble (CAT, *cable address translation*)	Sous-fonction du portail CAP, une traduction CAT traduit les adresses se trouvant dans le côté WAN-Data du portail CAP en adresses implantées dans un sous-réseau logique unique du côté LAN-Trans.
Traversée	Sous-fonction du portail CAP qui transfère en transparence les paquets du côté WAN-Data du portail CAP au côté LAN-Pass.
Portail de gestion du câble (CMP, *cable gestion portal*)	Fonction qui fournit des interfaces entre la tête de réseau et la base de données du service portail.
Portail DHCP de câble (CDP, *cable DHCP portal*)	Fonctions d'information d'adresse (par exemple, celles qui sont transmises par protocole DHCP) incluant un serveur pour le secteur LAN et un client pour les secteurs WAN.
Portail de nommage du câble (CNP, *cable naming portal*)	Portail qui fournit un service DNS simple pour les dispositifs IP de réseau LAN qui nécessitent des services de nommage.
Portail d'essai du câble (CTP, *cable testing portal*)	Portail qui permet d'initialiser à distance des validations par écho et des bouclages au sein du réseau LAN.

Tableau 5-3/J.191 – Description de la fonction de client de gestion

Fonctions de client de gestion	Description
Client DHCP de dispositif IP de réseau LAN	La fonction de client DHCP par câble est un composant résidentiel qui est utilisé pendant le processus d'approvisionnement de dispositif IP de réseau LAN afin de demander de façon dynamique les adresses IP et les autres informations de configuration d'élément logique.
Répondeur de bouclage de dispositif IP de réseau LAN	Au sein d'un dispositif IP de réseau LAN, le répondeur de bouclage renvoie en boucle, vers la fonction de bouclage du portail CTP, les données issues de la fonction de bouclage du portail CTP.

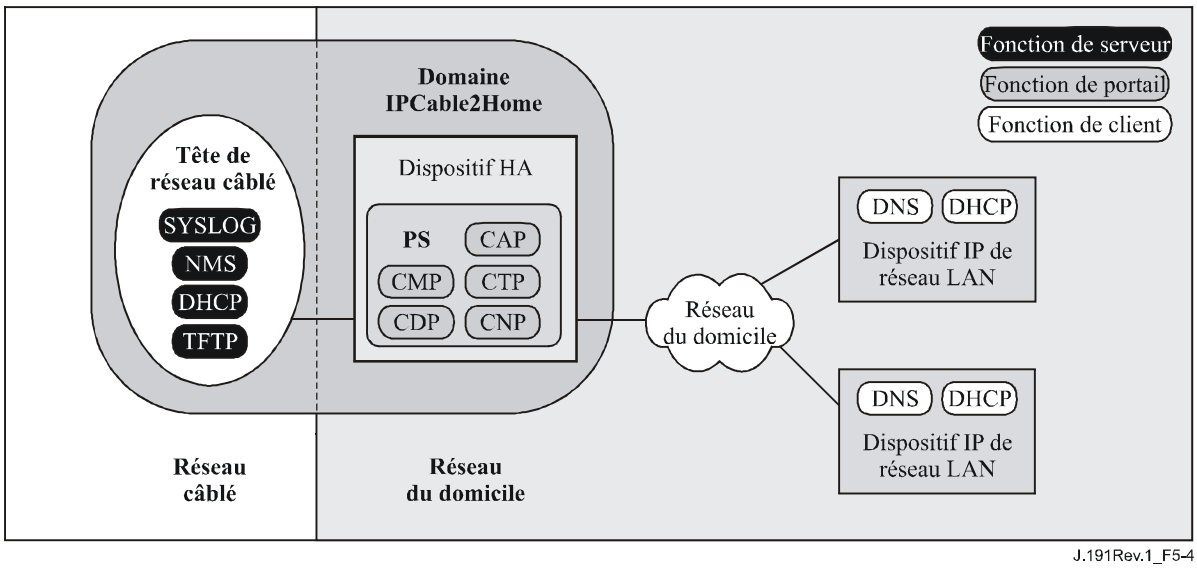


Figure 5-4/J.191 – Eléments de gestion

5.2.2 Fonctions de sécurité

Afin de prendre en charge les exigences de sécurité du système IPCable2Home, deux classes de fonctions de sécurité sont définies comme suit:

- fonctions de serveur de sécurité (Kerberos, centre de distribution de clés);
- fonctions de portail de sécurité.

Les fonctions de serveur de sécurité sont implantées dans la tête de réseau (HE) et les fonctions de portail de sécurité émulent des fonctions de client résidant à l'intérieur du service PS. Des exemples de fonctions de serveur de sécurité et de portail de sécurité sont présentés dans les Tableaux 5-4 et 5-5 puis sont illustrés par la Figure 5-5.

Tableau 5-4/J.191 – Description de la fonction PS de sécurité

Fonctions portail de sécurité	Description
Portail de sécurité de câble (CSP, *cable security portal*)	Le portail CSP communique avec les serveurs de sécurité de la tête de réseau. Il contient des fonctions qui assurent la participation du côté client aux processus d'authentification, d'échange de clés et de gestion de certificat qui sont définis par IPCable2Home. D'autres fonctions de sécurité sont la sécurité des messages de gestion, la participation aux processus de téléchargement sécurisés et la télégestion des pare-feu.
Pare-feu (FW, *firewall*)	Le pare-feu offre une fonctionnalité qui protège le réseau du domicile des attaques malveillantes.

Tableau 5-5/J.191 – Description de la fonction de serveur de sécurité

Fonctions de serveur de sécurité	Description
Serveurs de centre KDC de la tête de réseau	Dans la tête de réseau, les serveurs de centre KDC fournissent au portail CSP des services de sécurité et comportent des fonctions qui participent aux processus d'authentification et d'échange de clés définis par IPCable2Home.

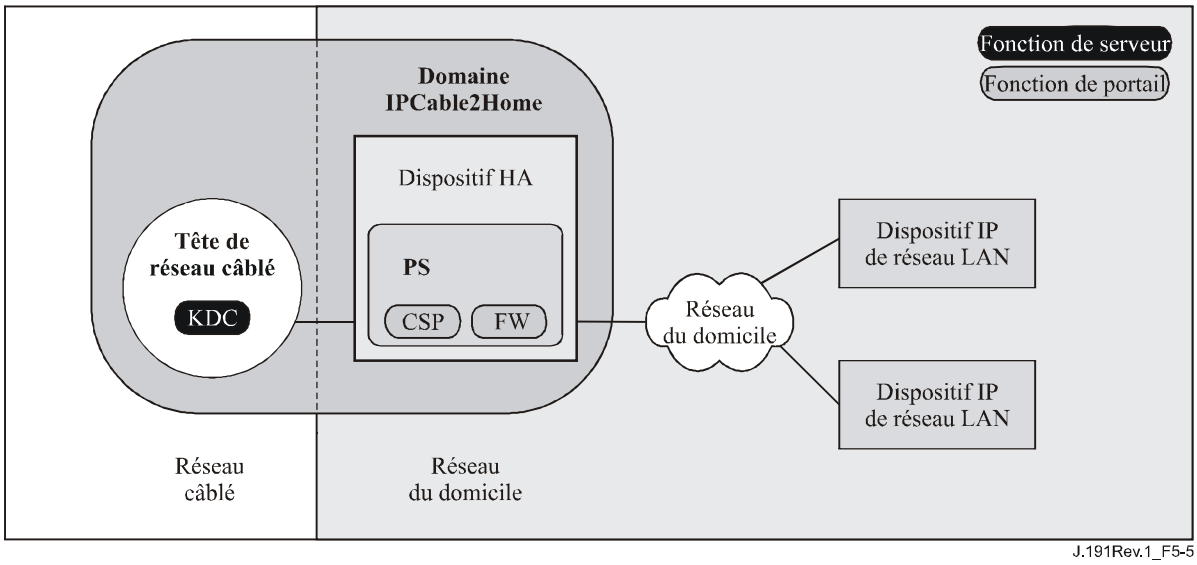


Figure 5-5/J.191 – Eléments de sécurité

5.2.3 Fonctions de qualité de service

L'architecture de qualité de service se compose d'une seule entité fonctionnelle fondée sur le service portail, qui est appelée *portail de qualité de service du câble* (CQP, *cable QoS portal*). Le portail CQP assure un transport transparent de la messagerie de qualité de service entre les applications IPCablecom et l'infrastructure de qualité de service IPCablecom sur le réseau câblé.

5.3 Modèle d'interface de messagerie IPCable2Home

Les communications entre les fonctions contenues dans les éléments de réseau et les dispositifs IP de réseau LAN passent par les interfaces de messagerie. Les types d'interfaces de messagerie sont différenciés par les éléments impliqués dans la communication. Les interfaces de messagerie sont illustrées par la Figure 5-6.

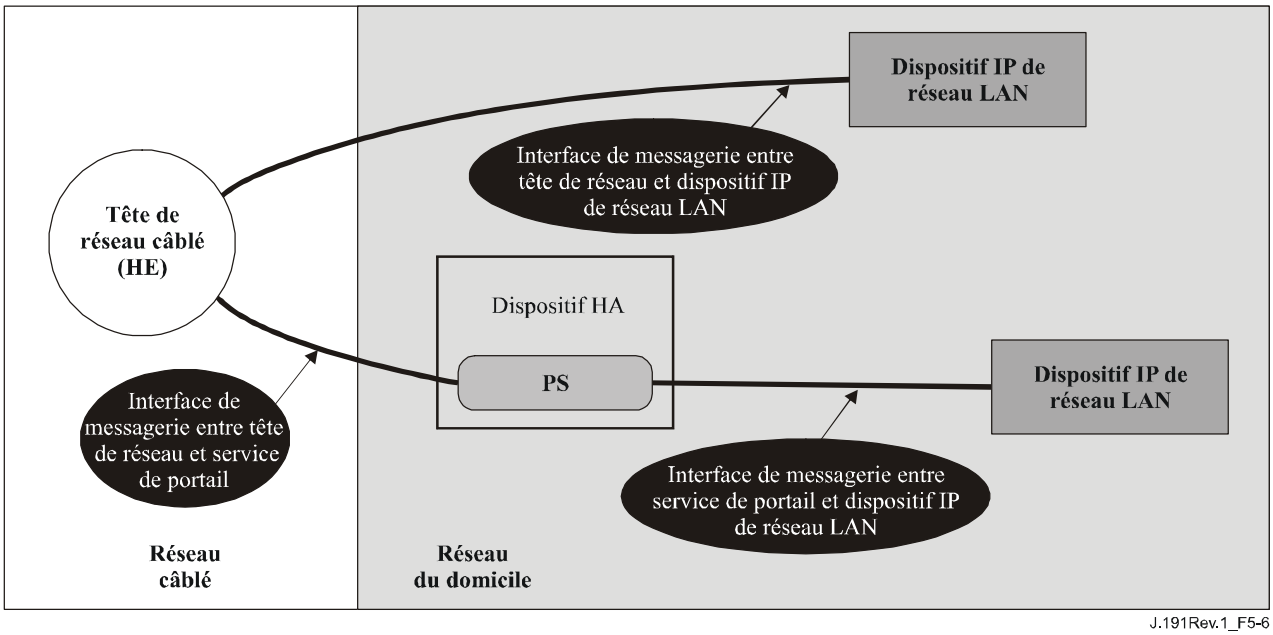


Figure 5-6/J.191 – Interfaces de référence

Les interfaces de messagerie IPCable2Home sont récapitulées dans le Tableau 5-6.

Tableau 5-6/J.191 – Chemins d'interface valables pour chaque fonctionnalité

Fonction	Protocole	Interface entre:		
		HE et PS	HE et disp. IP de réseau LAN	PS et disp. IP de réseau LAN
Service de nommage	DNS	Non spécifiée	Non spécifiée	Spécifiée dans la présente Recommandation
Téléchargement de logiciel	TFTP	Spécifiée dans la présente Recommandation	Non spécifiée	Non spécifiée
Acquisition d'adresse	DHCP	Spécifiée dans la présente Recommandation	Non spécifiée	Spécifiée dans la présente Recommandation
Gestion (simple) (en masse)	SNMP TFTP	Spécifiée dans la présente Recommandation Spécifiée dans la présente Recommandation	Non spécifiée	Non spécifiée

Tableau 5-6/J.191 – Chemins d'interface valables pour chaque fonctionnalité

Fonction	Protocole	Interface entre:		
		HE et PS	HE et disp. IP de réseau LAN	PS et disp. IP de réseau LAN
Notification d'événement	SNMP SYSLOG	Spécifiée dans la présente Recommandation Spécifiée dans la présente Recommandation	Non spécifiée	Non spécifiée
Qualité QS	Protocoles de QS IPCablecom	Non spécifiée	IPCablecom	Non spécifiée
Sécurité (distribution de clés)	Kerberos	Spécifiée dans la présente Recommandation	Non spécifiée	Non spécifiée
Sécurité (authentification)	Kerberos	Spécifiée dans la présente Recommandation	Non spécifiée	Non spécifiée
Validation par écho	ICMP	Spécifiée dans la présente Recommandation	Non spécifiée	Spécifiée dans la présente Recommandation
Bouclage/Echo	UDP/TCP	Non spécifiée	Non spécifiée	Spécifiée dans la présente Recommandation

5.4 Modèle de référence d'information IPCable2Home

Le fonctionnement du modèle de gestion se fonde sur un stockage d'informations maintenu dans le portail par les diverses fonctions PS (CAP, CDP, CMP, etc.). Ces fonctions doivent être en mesure d'interagir par échange d'informations et la base de données du portail est une entité conceptuelle qui représente la mémoire de ces informations. La base de données du portail ne constitue pas en elle-même une base de données spécifiée proprement dite, mais plutôt un outil pour aider à comprendre quelles informations sont échangées entre les divers éléments.

La Figure 5-7 montre les relations entre la base de données et les fonctions PS; le Tableau 5-7 décrit les informations typiquement associées à chacune de ces fonctions. La Figure 5-8 donne un exemple détaillé de l'implémentation indiquant l'ensemble des informations, les fonctions d'où découlent ces informations, et les relations entre fonctions et informations.

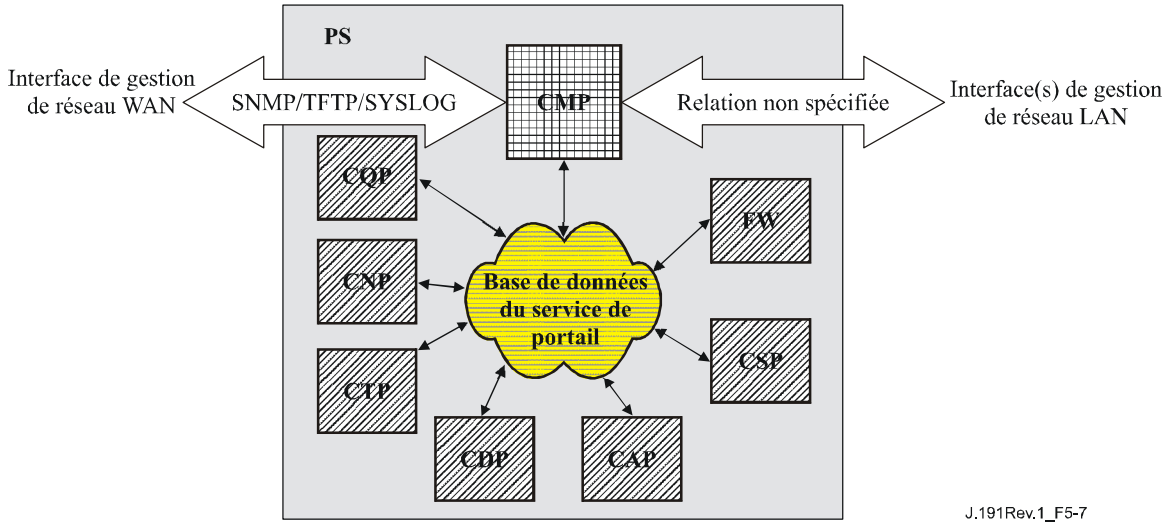


Figure 5-7/J.191 – Relations entre fonction PS et base de données du service portail

La base de données du service portail mémorise une multitude de relations entre données. Le portail CMP fournit l'interface de gestion de réseau WAN (SNMP) à la base de données du portail. Les fonctions remplies au sein du portail entrent et révisent les relations entre données dans la base de données du portail. De plus, les fonctions remplies au sein du portail peuvent restaurer des informations en provenance de la base de données de portail qui est entretenue par d'autres fonctions contenues dans le service portail.

Tableau 5-7/J.191 – Exemples typiques d'informations de base de données de portail

Nom	Usage (en général)
Informations CDP	Informations associées aux adresses acquises et attribuées par protocole DHCP
Informations CAP	Informations associées aux mappages de traduction d'adresses IPCable2Home
Informations CMP	Informations associées à l'état des fonctions de gestion
Informations CTP	Informations associées aux résultats des essais de réseau LAN effectués par le portail CMP
Informations CNP	Informations associées à la résolution de nom de dispositif IP de réseau LAN
Informations USFS	Informations associées à la fonction de commutateur de transmission sélective de sens montant
Informations CSP	Informations associées à l'authentification, à l'échange de clés, etc.
Informations de pare-feu	Informations associées au comportement du pare-feu (ensemble de règles) et à la connexion du pare-feu
Informations d'événement	Informations associées à la connexion locale pour tous les événements généraux, les transferts automatiques, etc.

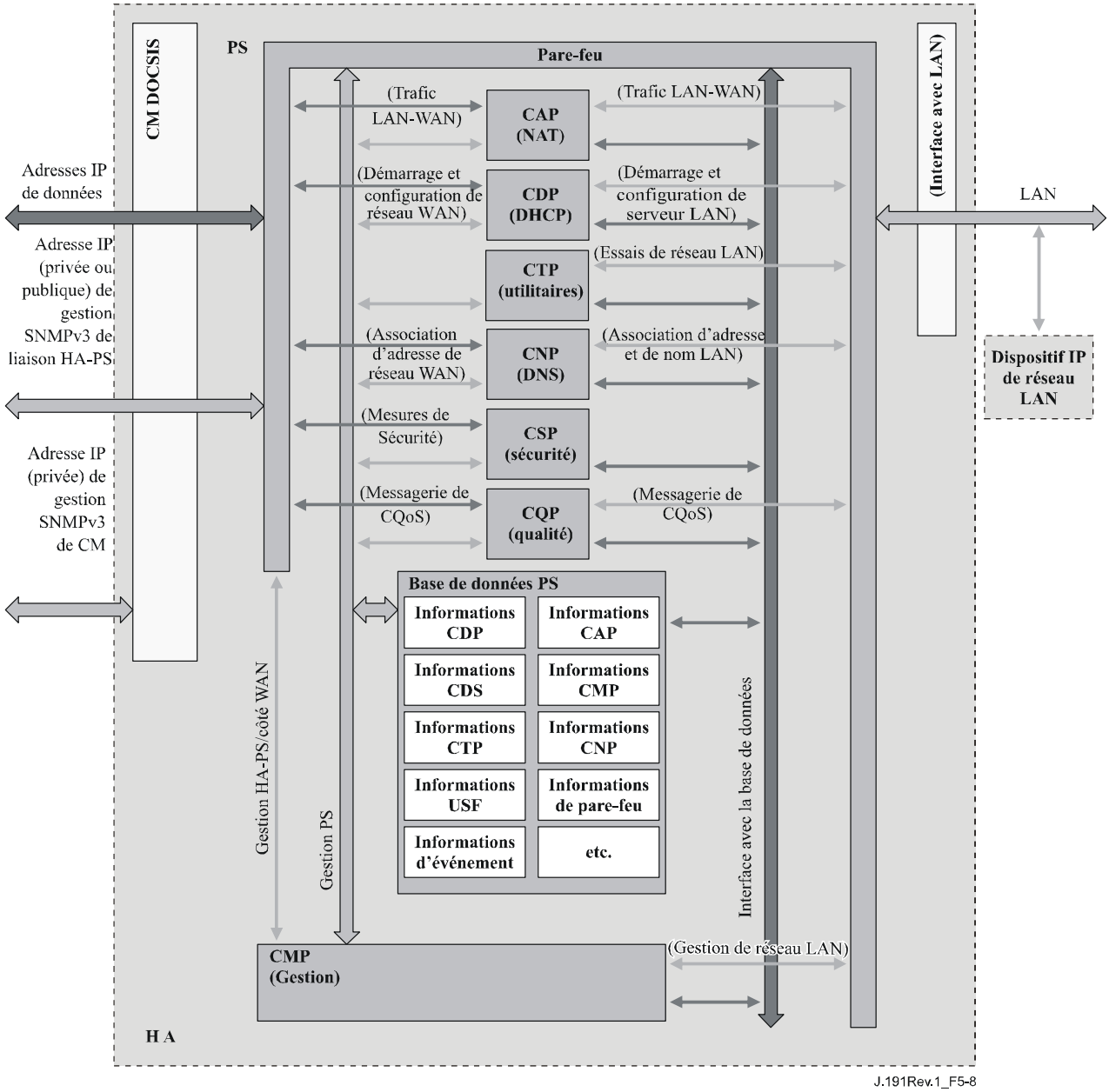


Figure 5-8/J.191 – Exemple détaillé d'implémentation d'une base de données de services portail

Le portail est géré à partir du réseau WAN via le portail CMP: dans une large mesure, cela implique l'accès aux informations de la base de données du portail. La gestion sert à l'initialisation et à l'approvisionnement des éléments de réseau du côté WAN, et aux diagnostics ou aux états du côté LAN. Les diagnostics peuvent s'appuyer sur le portail CTP afin d'obtenir une meilleure visibilité sur l'état en cours du réseau LAN. On peut mesurer la connexité et des performances rudimentaires du réseau.

Le portail CNP est le gestionnaire du système de dénomination de domaine (DNS, *domain name system*) du réseau LAN. Tous les dispositifs IP de réseau LAN de type LAN-Trans sont configurés par le portail CDP afin qu'ils utilisent le portail CNP comme serveur de nom primaire. Le portail CNP résout les noms de serveurs textuels des dispositifs IP de réseau LAN, retourne leurs adresses IP correspondantes et, en plus, renvoie les dispositifs IP de réseau LAN vers des serveurs DNS externes pour les demandes auxquelles les informations locales ne permettent pas de répondre.

Le portail CDP contient les fonctions d'adresse nécessaires pour prendre en charge le serveur DHCP dans le secteur LAN-Trans et un client DHCP dans les secteurs de réseau WAN.

Le portail CAP crée des mappages de traduction d'adresse entre les secteurs d'adresses WAN-Data et LAN-Trans. Le portail CAP est aussi responsable des décisions de commutation de transmission sélective de sens montant afin de préserver la largeur de bande du canal en amont du réseau HFC (WAN) du seul trafic du réseau LAN local. Enfin, le portail CAP contient la fonction de traversée, qui dérive le trafic entre les secteurs d'adresses du réseau LAN et du réseau WAN.

Le portail CSP fournit les capacités d'authentification du service portail ainsi que les activités d'échange de clés.

Le portail CQP fait partie d'un système qui active la qualité de service (QS) IPCablecom au moyen du service portail. Le portail CQP, agissant comme un pont transparent, réexpédie les messages de qualité de service conformes à IPCablecom entre applications IPCablecom et l'infrastructure de qualité de service IPCablecom.

5.5 Modèles fonctionnels IPCable2Home

La fonctionnalité de l'élément Services PS est compatible avec diverses infrastructures de réseau câblé, prises en charge par un certain nombre de différents modes opérationnels du service portail qui permettent au service PS de fonctionner correctement à l'intérieur d'une infrastructure à câblo-modems, ainsi qu'à l'intérieur d'une infrastructure IPCable2Home étendue. Celle-ci se fonde sur les infrastructures à câblo-modems afin d'activer des services additionnels et comprend un certain nombre de capacités qui sont semblables à celles qui se trouvent dans un système d'approvisionnement IPCablecom.

Pour les besoins de la configuration, le service portail peut fonctionner dans un des deux modes d'approvisionnement suivants:

- le mode d'approvisionnement DHCP;
- le mode d'approvisionnement SNMP.

Si le service PS ne reçoit pas les informations requises afin de déterminer le mode d'approvisionnement, il fonctionne en *mode IPCableHome inactif* avec une fonctionnalité réduite.

Lorsque le service portail fonctionne dans le mode d'approvisionnement DHCP, il peut fonctionner dans l'un des deux sous-modes de gestion de réseau suivants:

- mode d'accès NmAccess;
- mode de coexistence.

La Figure 5-9 illustre les divers modes de fonctionnement du service portail ainsi que les déclencheurs qui leur sont associés. Voir § 6.3.6.1.1.

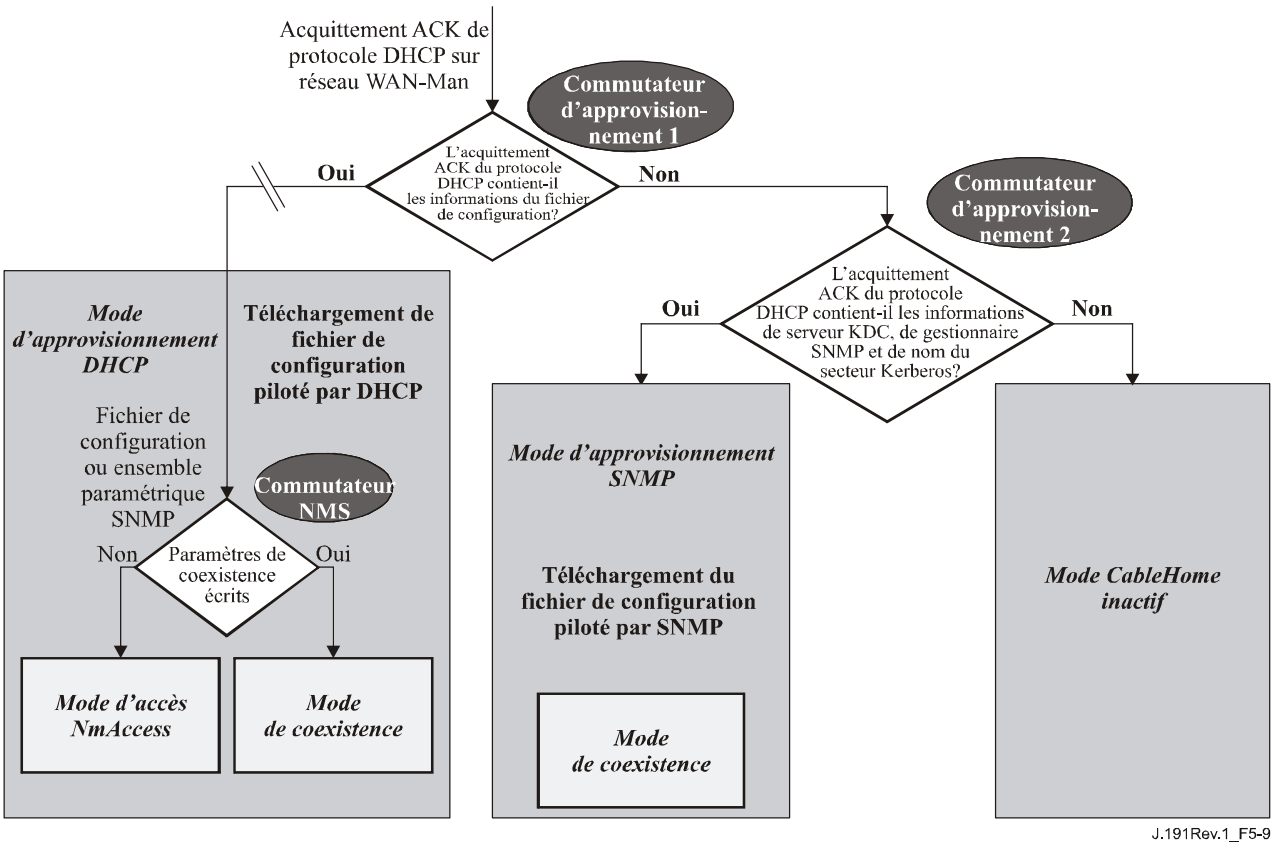


Figure 5-9/J.191 – Modes de fonctionnement du service portail

Si les informations du fichier de configuration PS (emplacement du serveur et nom de fichier) sont fournies et si les informations relatives au serveur Kerberos ne sont pas fournies au service portail dans le message ACK du protocole DHCP envoyé par le serveur DHCP du réseau câblé, le service portail fonctionne en mode d'approvisionnement DHCP. Lorsqu'il est en mode d'approvisionnement DHCP, le service portail peut fonctionner dans un des deux modes de gestion de réseau (accès NmAccess et coexistence). Dans le mode d'approvisionnement DHCP, le service portail fonctionne par défaut en mode de gestion de réseau NmAccess mais peut être configuré par le système NMS de façon à fonctionner en mode de coexistence.

Si les informations relatives au serveur Kerberos sont fournies et si les informations du fichier de configuration PS ne sont pas fournies au service portail dans le message ACK du protocole DHCP envoyé par le serveur DHCP du réseau câblé, le service portail fonctionne en mode d'approvisionnement SNMP. Lors du fonctionnement en mode d'approvisionnement SNMP, les informations et déclencheurs pour le téléchargement du fichier de configuration PS sont fournis par le système NMS au moyen de messages SNMP. A la différence du mode d'approvisionnement DHCP, le comportement de gestion de réseau ne change pas dans ce mode.

Si la combinaison erronée des informations de serveur Kerberos et de fichier de configuration PS est fournie au service PS dans le message ACK du protocole DHCP envoyé par le serveur DHCP du réseau câblé, le service portail passe par défaut au fonctionnement en mode CableHome inactif. Dans ce dernier mode, le service portail utilise les paramètres de configuration qui sont mémorisés localement. Si le service portail n'a jamais été préconfiguré, il fonctionne avec les paramètres par défaut de l'usine.

Le Tableau 5-8 décrit les infrastructures dans lesquelles chaque mode du service PS est destiné à fonctionner.

Tableau 5-8/J.191 – Infrastructures du service portail

Mode	Fonctionnalité directement affectée	Infrastructure prévue
Mode d'approvisionnement SNMP	Téléchargement du fichier de configuration	Infrastructure IPCable2Home étendue
Mode d'approvisionnement DHCP	Téléchargement du fichier de configuration	Infrastructures DOCSIS 1.0 et 1.1
Mode d'approvisionnement DHCP: mode d'accès NmAccess	Version SNMP utilisée entre NMS et PS	Infrastructure DOCSIS 1.0 (SNMP v1/v2)
Mode d'approvisionnement DHCP: mode de coexistence SNMP	Version SNMP utilisée entre NMS et PS	Infrastructures DOCSIS 1.1 et IPCable2Home étendue (SNMP v3)
Mode CableHome inactif	Gérabilité du protocole SNMP à partir de l'interface avec un réseau WAN	Toute infrastructure de réseau câblé ne prenant pas en charge l'approvisionnement et la gestion CableHome.

5.6 Interfaces physiques IPCable2Home

Il existe de nombreux types d'interfaces physiques qui peuvent être implémentées dans un dispositif contenant une fonctionnalité PS. Plusieurs de ces interfaces sont décrites dans la liste ci-dessous:

- interfaces de mise en réseau WAN, qui comprennent l'interface radioélectrique (RFI, *radio frequency interface*) qui est décrite par la Rec. UIT-T J.112 (ou Rec. UIT-T J.122) dans le cas du service portail imbriqué ainsi que, dans le cas du service portail autonome, d'autres interfaces de mise en réseau WAN destinées à la connexion avec un réseau WAN;
- interfaces de mise en réseau LAN, destinées à la connexion avec des dispositifs IP de réseau LAN;
- interfaces d'essai de matériel, telles que les interfaces du groupe JTAG et d'autres approches propres à des vendeurs, qui font partie des circuits intégrés et qui ne possèdent pas toujours les commandes logicielles nécessaires pour découpler ces interfaces. Celles-ci sont des automates matériels qui restent passifs jusqu'à ce que leurs lignes d'entrée soient pointées par des données. Bien qu'elles puissent servir à lire et à écrire des données, ces interfaces nécessitent une connaissance intime des circuits intégrés et de l'arrangement de la carte imprimée, de sorte qu'elles sont difficiles à "attaquer". Des interfaces d'essai de matériel PEUVENT être présentes dans un dispositif implémentant une fonctionnalité de services PS mais NE DOIVENT PAS être étiquetées ni décrites comme étant à l'usage du client;
- interfaces d'accès de gestion, également appelées *connecteurs de console*, qui sont des voies de communication (habituellement à la norme RS-232 mais qui peuvent être de type Ethernet, etc.) associées à un logiciel de débogage interactif avec un utilisateur qui est invité par le logiciel à introduire des données. Le logiciel accepte les ordres de lecture et d'écriture de données dans le service portail. Si le logiciel de cette interface est désactivé, la voie de communication physique l'est également. Un service PS NE DOIT PAS autoriser l'accès à des fonctions PS par l'intermédiaire d'une interface d'accès de gestion. L'accès aux fonctions PS DOIT être autorisé au moyen d'interfaces spécifiquement prescrites par la présente Recommandation, p. ex. par un accès commandé par l'opérateur en protocole SNMP;
- interfaces de diagnostic en lecture seulement, qui peuvent être implémentées de nombreuses façons et qui servent à offrir aux utilisateurs d'utiles informations de débogage, de dépannage et d'état du service PS. Celui-ci PEUT avoir des interfaces de diagnostic en lecture seulement;

- certains produits peuvent opter pour l'implémentation de fonctions dans les couches supérieures (comme des fonctions de réseau de transmission de données dans les locaux de clientèle), ce qui peut nécessiter une configuration par l'utilisateur. Un service portail PEUT offrir la possibilité de configurer des fonctions autres que de type IPCable2Home. L'accès à des fonctions PS par une interface de gestion (lecture/écriture) utilisant le mécanisme servant à configurer des fonctions autres que de type IPCable2Home NE DOIT PAS être autorisé.

6 Utilitaires de gestion

6.1 Introduction/Aperçu général

Les utilitaires de gestion offrent au câblo-opérateur les fonctions qui lui permettent de gérer et de configurer l'élément de Services PS, ainsi que d'effectuer des diagnostics à distance sur des dispositifs IP de réseau LAN. Le présent paragraphe décrit et spécifie les exigences pour ces capacités.

6.1.1 Objectifs

Les objectifs des utilitaires de gestion sont les suivants:

- fournir aux câblo-opérateurs la visibilité sur les dispositifs IP de réseau LAN;
- fournir aux câblo-opérateurs un ensemble minimal d'utilitaires de diagnostic qui leur permettront de vérifier la connexité entre les éléments de services portail et tout utilitaire IP de réseau LAN situé dans le secteur d'adresses LAN-Trans;
- fournir aux câblo-opérateurs, via les bases MIB, l'accès à des données internes de l'élément PS, permettre au câblo-opérateur de surveiller des paramètres spécifiés et de configurer ou reconfigurer, le cas échéant, des capacités spécifiées;
- permettre de signaler les exceptions et autres événements sous la forme de transferts du protocole SNMP, de messages vers un journal local, ou de messages vers un journal du système (SYSLOG) dans le réseau câblé.

6.1.2 Hypothèses

Les hypothèses sur l'environnement de gestion de réseau sont les suivantes:

- les dispositifs compatibles implémentent la suite protocolaire du protocole Internet (IPv4);
- le protocole SNMP est utilisé pour l'échange de messages de gestion entre le système NMS du réseau câblé et le service PS contenu dans le dispositif d'accès HA. Le protocole SNMP donne au système NMS la visibilité sur les interfaces avec le service PS au moyen de l'accès aux données internes du portail et par l'intermédiaire des bases MIB nécessaires;
- l'une quelconque des versions v1/v2c/v3 du protocole SNMP peut être utilisée comme protocole de gestion entre le système NMS et l'élément de services PS;
- les dispositifs IP de réseau LAN implémentent un client du protocole DHCP;
- les informations acquises au travers de l'échange de messages DHCP DISCOVER, DHCP REQUEST et DHCP OFFER entre le service portail et les dispositifs IP de réseau LAN, ainsi que les informations disponibles en provenance de la base de données du service portail (voir § 5.4) à travers la base MIB du groupe d'interfaces, sont suffisantes pour procurer au câblo-opérateur les connaissances nécessaires au sujet des dispositifs IP du réseau LAN;
- l'élément PS et les dispositifs IP de réseau LAN acceptent le protocole ICMP;

- l'utilitaire de groupeur PING fournit des fonctionnalités suffisantes pour donner au câblo-opérateur les informations nécessaires sur la connexité entre l'élément PS et les dispositifs IP de réseau LAN.

6.2 Architecture de gestion

6.2.1 Directives pour la conception du système

La liste des directives pour la conception du système d'utilitaires de gestion figure dans le Tableau 6-1. Cette liste donne des indications sur la mise au point des spécifications relatives aux utilitaires de gestion.

Tableau 6-1/J.191 – Directives pour la conception du système d'utilitaires de gestion

Référence	Directives pour la conception du système d'utilitaires de gestion
Mgmt 1	Le service PS implémentera la version SNMPv1/v2c/v3 pour fournir l'accès aux données internes des services PS.
Mgmt 2	Le service PS sera capable d'envoyer une commande ICMP de validation par écho à tout dispositif IP de réseau LAN spécifié dans le secteur LAN-Trans à destination du système NMS du réseau câblé et de mémoriser les résultats dans la base de données des services PS. Les résultats des essais de validation par écho sont accessibles par les objets de base MIB de portail CTP suivants: cabhCtpPingStatus, cabhCtpPingNumSent et cabhCtpPingNumRecv.
Mgmt 3	Le service PS sera capable d'exécuter un essai de vitesse de connexion avec un dispositif IP de réseau LAN spécifié dans le secteur LAN-Trans à destination du système NMS du réseau câblé et de mémoriser les résultats dans la base de données des services PS.
Mgmt 4	L'élément PS sera capable de signaler les événements.

6.2.2 Description du système d'utilitaires de gestion

Comme indiqué à la Figure 6-1, l'architecture des utilitaires de gestion comporte les composants suivants:

1) le portail de gestion du câble (CMP, *cable management portal*);
2) le portail d'essai du câble (CTP, *cable test portal*);
3) un mécanisme de rapport d'événements au sein du portail CMP;
4) un système de gestion de réseau (NMS, *network management system*) du protocole SNMP qui fait partie du réseau câblé.

Le système NMS du réseau câblé surveille et configure le service portail en accédant à la base de données du service portail à travers les bases MIB spécifiées au § 6.3.7. Le système NMS peut aussi communiquer directement avec les dispositifs IP de réseau LAN situés dans le secteur LAN-Pass.

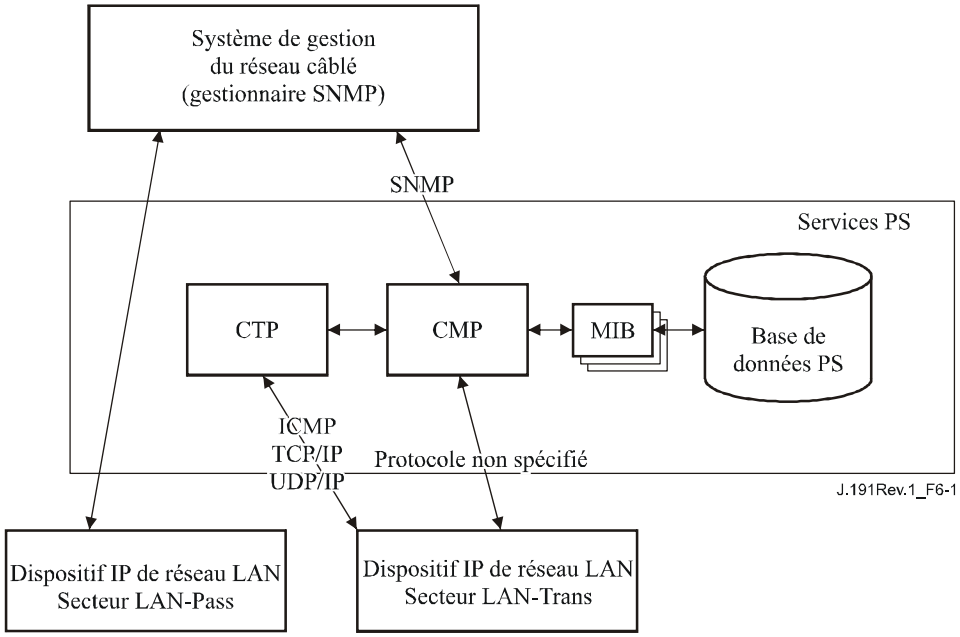


Figure 6-1/J.191 – Architecture de gestion

Les éléments fonctionnels CMP et CTP résident au sein du service portail. L'élément logique PS peut être imbriqué ou autonome, en termes de fonctionnalité de câblo-modem, comme décrit au § 5.

Dans les deux cas (PS imbriqué et PS autonome), le câblo-modem et le service PS sont – du point de vue de la gestion – des entités de gestion séparées et indépendantes: il n'y a pas de partage de données entre CM et PS, sauf dans le cas d'un téléchargement d'image logicielle vers un service PS imbriqué, où l'on accède aux objets docsDevSoftware du câblo-modem afin d'établir, d'initialiser et de surveiller le téléchargement d'une unique image logicielle combinée. A cause de cette indépendance de gestion, le câblo-modem et le service portail DOIVENT répondre à des adresses IP de gestion différentes et indépendantes. Les objets de base MIB du câblo-modem ne sont visibles que lorsque le gestionnaire y accède par l'adresse IP de gestion du câblo-modem. Ils ne sont pas visibles via l'adresse IP de gestion du service portail (et vice versa). Les droits d'accès du protocole SNMP aux entités PS et CM doivent être établis indépendamment, ce qui n'empêche pas d'utiliser un agent SNMP unique dans le cas d'un service PS imbriqué.

L'élément de services PS accepte les protocoles SNMPv1, SNMPv2c et SNMPv3. Le § 5.5 a présenté les deux modes d'approvisionnement acceptés par un élément de services PS et le § 7 donne des détails supplémentaires sur ces modes. Le mode d'approvisionnement dans lequel le service PS fonctionne détermine partiellement la version du protocole SNMP qui est utilisée par le service PS. Des détails supplémentaires figurent au § 6.3.3.

6.3 Le portail de gestion du câble (CMP)

Le portail de gestion du câble (CMP) existe au sein du service PS. Il sert de concentrateur des commandes de gestion pour les accès de gestion du côté WAN. Le portail CMP agrège et interconnecte les informations de gestion dans les secteurs WAN-MAN et LAN-Trans parce qu'ils ne sont pas directement accessibles de l'un à l'autre.

6.3.1 Objectifs du portail CMP

Les objectifs du portail de gestion du câble sont les suivants:

- permettre au système NMS de voir et de mettre à jour les informations de configuration du portail d'adresse câble (CAP);

- permettre au système NMS de voir et de mettre à jour les informations de configuration du pare-feu;
- permettre une validation par écho pour les dispositifs IP de réseau LAN se trouvant dans le secteur LAN-Trans, via le portail d'essai du câble (CTP);
- permettre de voir les informations de dispositif IP de réseau LAN obtenues via le portail DHCP du câble (CDP);
- permettre de voir les résultats de la surveillance de la performance de dispositif IP de réseau LAN, assurée par le portail d'essai du câble (CTP);
- permettre au système NMS d'accéder à d'autres paramètres de configuration du service PS;
- traiter en masse les commandes SNMP passées à partir du système NMS de réseau câblé dans un fichier de configuration PS;
- contribuer à la sécurité en donnant accès aux paramètres de sécurité et à l'utilisation de la version SNMPv1/v2c/v3 dans le mode de gestion de réseau approprié;
- offrir la possibilité de désactiver des segments de réseau LAN.

6.3.2 Directives de conception du portail CMP

La liste des directives de conception du portail CMP sont énumérées dans le Tableau 6-2. Cette liste donne des indications pour la spécification des fonctions du portail CMP.

Tableau 6-2/J.191 – Directives de conception du portail CMP

Référence	Directives de conception du système de portail CMP
CMP 1	Les interfaces prendront en charge les caractéristiques et fonctions de gestion et de diagnostic nécessaires pour le traitement des services câblés approvisionnés dans le réseau du domicile.
CMP 2	La perte de connexion entre fournisseur(s) de service à haut débit et réseau du domicile ne désactivera ni ne dégradera le fonctionnement des fonctions internes d'établissement de réseau du domicile.
CMP 3	Le réseau du domicile se rétablira progressivement après une coupure de courant et les dispositifs connectés au réseau du domicile devront toujours revenir à l'état opérationnel où ils étaient avant la coupure.
CMP 4	Les dispositifs du réseau du domicile devront être faciles à installer et à configurer pour le fonctionnement, exactement comme un appareil d'utilisation résidentiel.

6.3.3 Description du système de portail CMP

Comme indiqué plus haut, le portail CMP sert de concentrateur des commandes de gestion pour les accès de gestion du côté WAN. Il interconnecte les éléments de gestion de réseau WAN et les éléments de réseau LAN après avoir agrégé les informations qui leur sont destinées.

Le portail CMP travaille dans l'un quelconque des trois modes de gestion de réseau.

Comme décrit au § 5.5, lorsque le service portail se trouve en mode d'approvisionnement SNMP, il fonctionne par défaut en mode de coexistence SNMPv3 sans activation des versions SNMPv1 et SNMPv2. Il utilise le serveur Kerberos afin de distribuer des matériaux de verrouillage par clés. Le modèle de sécurité fondé sur l'utilisateur (USM) [RFC 3414] et le modèle de commande d'accès fondé sur la vue (VACM) [RFC 3415] sont pris en charge afin que le câblo-opérateur puisse implémenter la politique de sécurité d'accès aux bases MIB spécifiées dans le système IPCable2Home.

Comme décrit au § 5.5, lorsque le service PS se trouve en mode d'approvisionnement DHCP, il fonctionne par défaut en mode NmAccessTable mais peut être configuré par le câblo-opérateur de façon à fonctionner en mode de coexistence SNMPv3. En mode NmAccessTable, l'accès de gestion est régi par l'élément NmAccessTable selon RFC 2669 et les protocoles SNMPv1/v2c sont acceptés. Si le service PS est configuré de façon à fonctionner en mode de coexistence SNMPv3, l'accès de gestion est régi comme décrit dans RFC 2576, les protocoles SNMPv1/v2c/v3 sont pris en charge, les modèles USM et VACM sont pris en charge et les matériaux de verrouillage par clés sont distribués au moyen des éléments RFC 2786 et des nuplets TLV contenus dans le fichier de configuration PS.

Si le service PS ne reçoit pas les paramètres de décision entre modes d'approvisionnement SNMP et DHCP et revient au mode CableHome inactif, il désactive l'accès SNMP à partir de ses interfaces avec le réseau WAN et répond à tout message SNMPv1 ou SNMPv2c reçu d'une quelconque interface avec le réseau LAN.

Le Tableau 6-3 contient les définitions des termes qui sont propres au portail CMP.

Tableau 6-3/J.191 – Définition des termes

Contrôle de gestion	Accès en lecture ou en écriture à un ensemble de paramètres qui contrôlent ou surveillent le comportement du service portail.
Base de données de services PS	Ensemble de paramètres qui contrôle ou surveille le comportement de l'élément de services PS, lisible par le système de gestion du réseau WAN. Il peut être conçu comme un répertoire d'informations décrivant l'état actuel du service portail.
Utilisateur	Comme défini dans le protocole SNMP [RFC 3414, section 2.1], un utilisateur possède un nom qui lui est associé, des définitions de sécurité associées et un accès à une vue.
Vue	Une vue est un ensemble d'objets de base MIB assortis des droits d'accès à ces objets. Chaque vue a un nom et est associée à un utilisateur [RFC 3415, section 2.4].
Autorisation ultime	Autorité unique qui établit, modifie ou supprime les identificateurs de l'utilisateur, les clés d'authentification, les clés de chiffrement et les droits d'accès à la base de données du service portail. Cet utilisateur est responsable de toutes les opérations de gestion de la sécurité.
Utilisateur de maintenance	Utilisateur qui n'effectue en principe que des opérations en lecture seule sur la base de données du service portail. Ces opérations servent surtout à effectuer la surveillance et la comptabilité.
Utilisateur-administrateur	Utilisateur qui effectue en principe à la fois des opérations de lecture et d'écriture sur la base de données du service portail. Ces opérations servent à la configuration et la gestion des dérangements.

Parmi les exemples de types d'informations manipulées via le contrôle de gestion sur le câble figurent l'établissement des politiques de pare-feu, les mappages des conversions NAT configurées selon le système NMS, l'initialisation d'utilitaires de diagnostic à distance et l'accès aux résultats, l'état du service portail, et la configuration du champ des adresses LAN. Ainsi qu'il sera montré plus loin, les diverses interfaces de messages de gestion peuvent disposer de droits d'accès à différents ensembles paramétriques. Il est possible d'accéder à la base de données du service portail aussi bien à partir du réseau WAN que du réseau LAN. Cependant l'accès par réseau LAN n'est pas spécifié. La Figure 6-2 indique trois interfaces de messages de gestion possibles:

- NMS – CMP: messages de gestion échangés entre le système NMS du réseau câblé et le portail CMP;
- CMP – dispositif IP de réseau LAN: échange de messages de gestion entre le portail CMP et des dispositifs IP de réseau LAN situés dans le secteur LAN-Trans (cette messagerie n'est pas spécifiée par IPCable2Home);

- NMS – dispositif IP de réseau LAN: échange de messages de gestion entre le système NMS du réseau câblé et des dispositifs IP de réseau LAN situés dans le secteur LAN-Pass (cette messagerie n'est pas spécifiée par IPCable2Home);
- NMS – dispositif IP de réseau LAN: échange de messages de gestion entre le système NMS du réseau câblé et des dispositifs IP de réseau LAN situés dans le secteur LAN-Trans (interface fournie par la configuration du portail CAP – voir § 8.3.2). Cette messagerie n'est pas spécifiée par IPCable2Home.

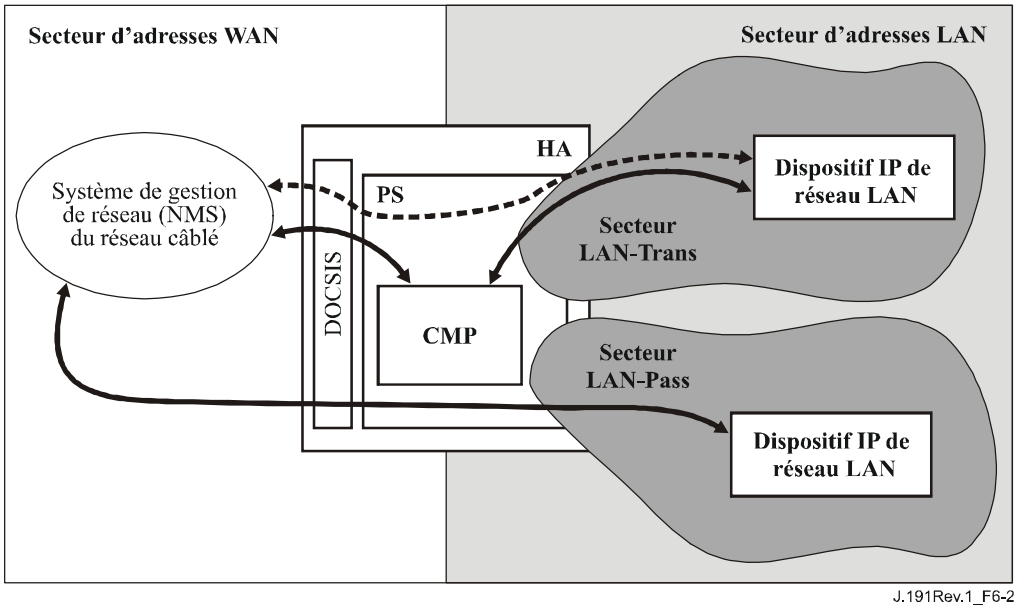


Figure 6-2/J.191 – Interfaces avec les messages de gestion

Le portail CMP est essentiellement une entité à laquelle on accède (au moyen du système NMS) par un réseau WAN et qui est contrôlée par un réseau WAN. De plus, on peut faire appel au portail CMP pour informer en tant que de besoin le système NMS du réseau câblé au sujet de fichiers de journalisation dans le système d'événements ou de transferts. Un exemple d'implémentation de portail CMP est illustré à la Figure 6-3 afin de présenter les concepts des fonctionnalités de portail CMP.

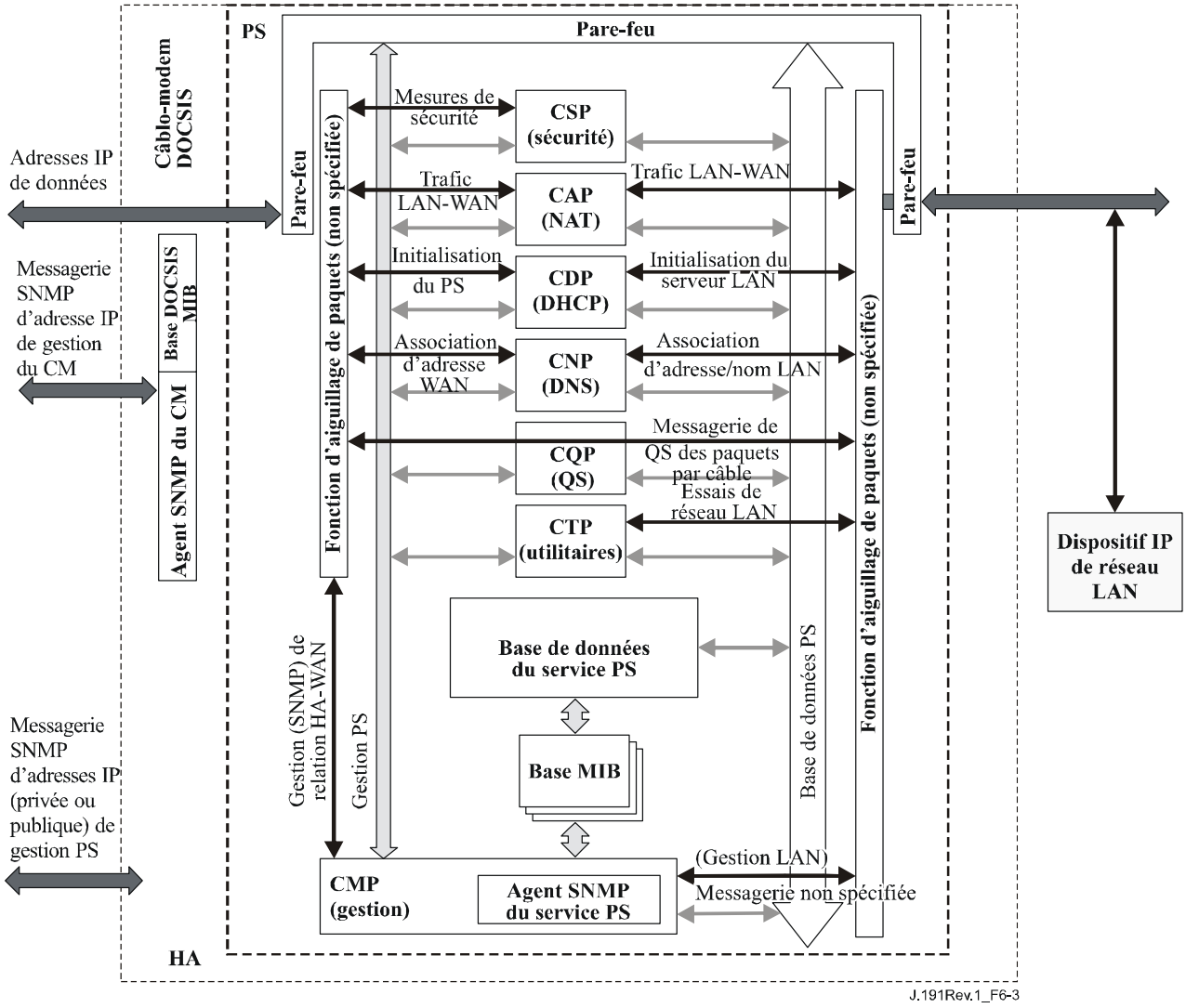


Figure 6-3/J.191 – Organigramme des services PS

Les utilitaires de gestion du système NMS utilisent le protocole SNMP pour accéder aux objets et les gérer dans le service portail. Si celui-ci fonctionne en mode de coexistence SNMPv3, ce protocole fournit à l'opérateur du système NMS l'authentification de l'utilisateur auprès du service portail, l'accès fondé sur la vue aux objets de la base d'informations de gestion (MIB, *management information base*) contenue dans le service portail, et le chiffrement des messages de gestion sur demande.

Le portail CMP est chargé d'établir le mappage de l'identificateur d'objet (OID, *object ID*) et de l'instance de l'identificateur OID pour tous les volets contenus dans les blocs fonctionnels du service portail, comme le portail CAP ou un stockage local tel que la base de données du service portail.

En plus du portail CMP, un opérateur de système NMS peut accéder directement aux dispositifs IP de réseau LAN ou les "gérer" en utilisant une adresse de traversée entre la tête de réseau et le dispositif de réseau LAN à gérer. Aucune règle ne prescrit cependant que les dispositifs IP de réseau LAN doivent répondre à de quelconques protocoles particuliers, que ces messages concernent ou non la gestion.

6.3.4 Exigences générales pour le portail CMP

Le service portail DOIT implémenter les types de messages ICMP d'écho et de réponse à l'écho (type 8 et type 0) ainsi que les types de messages ICMP de marqueur temporel et de réponse au

marqueur temporel (type 13 et type 14), comme décrit en RFC 792 et répondre correctement aux demandes de validation par écho reçues par une quelconque interface.

Si le service portail fonctionne en mode d'approvisionnement DHCP (indiqué par une valeur de "1" dans l'objet cabhPsDevProvMode), le portail CMP DOIT utiliser par défaut la version SNMPv1/v2c pour la messagerie de gestion échangée avec le système NMS et suivre les règles décrites au § 6.3.6.1 concernant les modes NmAccess et coexistence.

Si le service portail fonctionne en mode d'approvisionnement SNMP (indiqué par une valeur de "2" dans l'objet cabhPsDevProvMode), le portail CMP DOIT utiliser le protocole SNMPv3 pour la messagerie de gestion échangée avec le système NMS, conformément aux règles décrites au § 6.3.6.2.

Lorsque le service portail fonctionne en mode de coexistence SNMP, le réglage d'autorité ultime DOIT TOUJOURS être l'administrateur du réseau WAN (ou du service PS).

Lorsque le service portail fonctionne en mode CableHome inactif comme décrit au § 5.5 et au § 7.2.3.3 et comme indiqué par une valeur de "3" dans l'objet cabhPsDevProvMode, le service portail NE DOIT PAS accepter ou traiter un quelconque message SNMP reçu par l'intermédiaire d'une quelconque interface avec le réseau WAN.

Lorsque le service portail fonctionne en mode CableHome inactif comme décrit au § 5.5 et au § 7.2.3.3 et comme indiqué par une valeur de "3" dans l'objet cabhPsDevProvMode, le service portail DOIT accepter et traiter les messages SNMP reçus par l'intermédiaire d'une quelconque interface avec le réseau LAN conformément aux réglages de l'objet docsDevNmAccessTable (voir § 6.3.6.1) ou conformément aux réglages du modèle VACM (voir § 6.3.6.3).

La racine des bases MIB (PSDev, CAP, CDP, CTP et de sécurité) DOIT être "(enterprises.4491.2.4)".

Le service portail DOIT inclure dans l'objet "sysDescr" (d'après RFC 3418) – selon l'ordre spécifié ci-dessous – la version du matériel, le nom du vendeur, la version de l'image d'amorçage en mémoire morte, la version du logiciel et le numéro du modèle. Le format des informations spécifiquement contenues dans l'objet "sysDescr" DOIT être le suivant.

Information à signaler	*Format de chaque champ*
Version du matériel	HW_REV: <version du matériel>
Nom du vendeur	VENDOR: <nom du vendeur>
Mémoire morte d'amorçage	BOOTR: <version de mémoire d'amorçage>
Version du logiciel	SW_REV: <version du logiciel>
Numéro du modèle	MODEL: <numéro du modèle>

L'objet "sysDescr" DOIT être composé d'une liste de cinq paires de type/valeur entre doubles crochets. La séparation entre le type et la valeur est un caractère de deux points suivi d'un espace vide ": ". La séparation entre deux paires de type/valeur est un caractère de point-virgule suivi d'un espace vide "; ". Par exemple, l'objet sysDescr d'un service PS de vendeur X, de version de matériel 5.2, de version de mémoire morte d'amorçage 1.4, de version logicielle 2.2 et de numéro de modèle X se présentera comme suit:

texte quelconque<<HW_REV: 5.2; VENDOR: X; BOOTR: 1.4; SW_REV: 2.2; MODEL: X>> texte quelconque

Le service portail doit signaler, dans l'objet sysDescr, toutes les informations permettant de déterminer les versions de logiciel et de politique de pare-feu que le service PS est en mesure de prendre en charge. Si certains champs de l'objet sysDescr ne sont pas applicables, le service PS

DOIT signaler "NONE" comme valeur. Par exemple, un service portail sans BOOTR indiquera "BOOTR: NONE".

La valeur de l'objet de base MIB "docsDevSwCurrentVers" DOIT contenir les mêmes informations de version logicielle que celles qui sont incluses dans l'objet "sysDescr".

Lorsqu'un PS et un CM sont imbriqués dans le même dispositif, les objets sysDescr et docsDevSwCurrentVers du service PS DOIVENT signaler les mêmes valeurs que les objets du modem CM.

L'objet sysObjectID du groupe de système MIB-2 [RFC 3418] DOIT être implémenté et DOIT persister lors des réinitialisations de dispositif et des périodes d'alimentation.

L'objet sysUpTime du groupe de système MIB-2 [RFC 3418] DOIT être implémenté. SysUpTime est le temps écoulé depuis la réinitialisation du système.

L'objet sysContact du groupe de système MIB-2 [RFC 3418] DOIT être implémenté et DOIT persister lors des réinitialisations de dispositif et des périodes d'alimentation. SysContact retourne le nom de l'utilisateur ou de l'administrateur de système s'il est connu.

L'objet sysLocation du groupe de système MIB-2 [RFC 3418] DOIT être implémenté et DOIT persister lors des réinitialisations de dispositif et des périodes d'alimentation.

L'objet sysServices du groupe de système MIB-2 [RFC 3418] DOIT être implémenté et DOIT persister lors des réinitialisations de dispositif et des périodes d'alimentation.

L'objet sysServices DOIT renvoyer la valeur "3" (passerelle Internet) lorsqu'il est interrogé dans un élément de services PS.

L'objet sysName du groupe de système MIB-2 [RFC 3418] DOIT être implémenté et DOIT persister lors des réinitialisations de dispositif et des périodes d'alimentation. L'interrogation sysName retourne le nom du système.

Les objets du groupe de système MIB-2 autres que sysDescr, sysObjectID, sysUpTime, sysContact, sysName, sysLocation et sysServices NE DEVRAIENT PAS être implémentés.

La base MIB de groupe d'interfaces [RFC 2863] DOIT être implémentée conformément à l'Annexe A et aux prescriptions du § 6.3.8.

Le groupe SNMP de base MIB-2 [RFC 3418] DOIT être implémenté.

L'objet snmpSetSerialNo du groupe snmpSet [RFC 3418] DOIT être implémenté. L'objet snmpSetSerialNo est un verrou consultatif utilisé afin de permettre à plusieurs entités coopératives de protocole SNMPv2, agissant toutes comme gestionnaires, de coordonner leur utilisation du fonctionnement de l'ensemble SNMPv2.

Les objets de groupe snmpSet autres que snmpSetSerialNo NE DEVRAIENT PAS être implémentés.

Lorsque des objets de base MIB d'un élément de services PS sont réglés à leur valeur par défaut au moyen des bases MIB d'objet cabhCapSetToFactory, cabhCdpSetToFactory, cabhCtpSetToFactory ou cabhPsDevSetToFactory, la fonctionnalité PS correspondante DOIT utiliser les réglages par défaut d'usine sans devoir réapprovisionner l'élément de services PS.

6.3.5 Exigences du protocole SNMP

Les appels à commentaires suivants du groupe IETF DOIVENT être suivis ou implémentés selon le cas:

1) protocole simple de gestion de réseau [RFC 1157];
2) introduction au protocole SNMPv2 fondé sur la communauté [RFC 1901];
3) fonctionnement du protocole pour la version SNMPv2 [RFC 3416];

4) mappages de transport pour la version SNMPv2 [RFC 3417];

5) base d'informations de gestion pour la version 2 du protocole simple de gestion de réseau (SNMPv2) [RFC 3418];

6) introduction à la version SNMPv3 [RFC 3410];

7) base MIB du cadre du protocole SNMP [RFC 2571];

8) traitement et expédition de messages pour SNMP [RFC 3412];

9) base MIB des applications SNMP [RFC 3413];

10) groupe de base MIB snmpUSM [RFC 3414];

11) groupe de base MIB snmpVACM [RFC 3415];

12) base MIB de communauté SNMP [RFC 2576];

13) protocole SNMPv2-CONF.

Pour la prise en charge de la version SMIv2, les appels à commentaire suivants du groupe IETF DOIVENT être implémentés:

1) structure des informations gérées, version 2 (SMIv2) [RFC 2578];

2) conventions d'écriture pour SMIv2 [RFC 2579];

3) déclarations de conformité pour SMIv2 [RFC 2580].

6.3.6 Exigences relatives au mode de gestion de réseau

Le § 5.5 a présenté deux modes d'approvisionnement (DHCP et SNMP) et deux modes de gestion du réseau (NmAccessTable et coexistence avec SNMPv3), que le service PS est appelé à prendre en charge. Les § 7.2.3.3, 7.3.3.2 et 7.3.3.3 apportent des détails complémentaires au sujet du fonctionnement du service PS dans chacun des deux modes d'approvisionnement.

Le présent paragraphe décrit les règles applicables aux modes de gestion du réseau que le service portail est tenu de prendre en charge. Le § 6.3.6.1 et ses sous-paragraphes décrivent les modes de gestion du réseau pour un service portail fonctionnant en mode d'approvisionnement DHCP. Le § 6.3.6.2 et ses sous-paragraphes décrivent les modes de gestion du réseau pour un service portail fonctionnant en mode d'approvisionnement SNMP.

6.3.6.1 Modes de gestion de réseau pour un service PS fonctionnant en mode d'approvisionnement DHCP

Le service portail DOIT accepter les protocoles SNMPv1, SNMPv2c et SNMPv3 ainsi que Coexistence avec le protocole SNMP, comme décrit par les documents RFC 2576 et RFC 3414. Le service portail DOIT prendre également en charge le mode NmAccessTable comme défini par RFC 2669. La prise en charge des modes de gestion de réseau par un service portail fonctionnant en mode d'approvisionnement DHCP fait l'objet des directives suivantes:

6.3.6.1.1 Fonctionnement de base d'un service portail fonctionnant en mode d'approvisionnement DHCP

Le fonctionnement initial du service PS configuré pour le mode d'approvisionnement DHCP peut être considéré comme comportant trois étapes:

1) le comportement du service PS après qu'il ait été configuré pour le mode d'approvisionnement DHCP mais avant que son mode de gestion de réseau ait été configuré au moyen du fichier de configuration PS;

2) la détermination du mode de gestion du réseau;

3) le comportement du service PS après que son mode de gestion de réseau ait été configuré.

Les règles de fonctionnement de chacune de ces étapes sont les suivantes:

1) une fois que le service PS a été configuré de façon à fonctionner en mode d'approvisionnement DHCP (indiqué par une valeur cabhPsDevProvMode de "1" (DHCPmode)) mais avant qu'il ait été configuré pour un mode de gestion de réseau, le service PS DOIT fonctionner comme suit:
   - tous les paquets SNMP sont abandonnés;
   - aucune des bases MIB du protocole SNMPv3 (base MIB de communauté, base MIB de cible, base MIB de modèle VACM, base MIB de modèle USM, base MIB de notification) n'est accessible au gestionnaire SNMP contenu dans le système NMS;
   - aucun des éléments dans la base SNMP-USM-DH-OBJECTS-MIB n'est accessible au gestionnaire SNMP contenu dans le système NMS;
   - le fichier de configuration PS spécifié dans l'offre DHCP est téléchargé et traité;
   - le traitement réussi de tous les éléments de base MIB contenus dans le fichier de configuration PS DOIT être achevé avant le début du calcul des valeurs publiques dans la table usmDHKickstart;
2) si un service PS fonctionne en mode d'approvisionnement DHCP, le contenu du fichier de configuration PS détermine le mode de gestion du réseau comme décrit ci-dessous:
   - le service PS est en mode d'accès SNMPv1/v2c docsDevNmAccess si le fichier de configuration PS ne contient QUE l'objet docsDevNmAccessTable réglant la commande d'accès SNMP;
   - si le fichier de configuration PS ne contient pas d'éléments de commande d'accès du protocole SNMP (docsDevNmAccessTable ou snmpCommunityTable ou TLV 34.1/34.2 ou TLV38), le service portail est alors en mode NmAccess;
   - si le fichier de configuration PS contient le réglage snmpCommunityTable et/ou TLV type 34.1 et 34.2 et/ou TLV type 38, le service portail est alors en mode de coexistence SNMP. Dans ce cas, on ignore toutes les entrées introduites dans l'objet docsDevNmAccessTable;
3) après achèvement du processus d'approvisionnement décrit au § 13.2 (indiqué par la valeur 'pass' (1) dans l'objet cabhPsDevProvState), le service portail fonctionne dans l'un des deux modes de gestion. Le mode de gestion de réseau est déterminé par le contenu du fichier de configuration PS comme décrit ci-dessus. Les règles de fonctionnement du service PS pour chacun des deux modes de gestion de réseau sont les suivantes:

Mode NmAccess utilisant la version SNMPv1/v2c

- le service PS DOIT traiter les paquets SNMPv1/v2c et abandonner les paquets SNMPv3;
- la table docsDevNmAccessTable commande les destinations d'accès et de transfert comme décrit dans RFC 2669. Le service PS DOIT appliquer la politique d'accès de gestion qui est définie dans la table NmAccess pour tout accès aux objets de base MIB spécifiés, sans tenir compte de l'interface ou du protocole d'accès utilisé;
- aucune des bases MIB du protocole SNMPv3 (base MIB de communauté, base MIB de cible, base MIB de modèle VACM, base MIB de modèle USM, MIB de notification) n'est accessible.

Lorsque le service PS fonctionne en mode NmAccess du protocole SNMPv1/v2c, il DOIT prendre en charge la capacité d'envoyer des transferts automatiques comme spécifié par l'objet de base MIB suivant (extension de base MIB proposée pour la table docsDevNmAccess):

```
DocsDevNmAccessTrapVersion OBJECT-TYPE
SYNTAX INTEGER {
```

DisableSNMPv2trap(1),

EnableSNMPv2trap(2),

}

MAX-ACCESS read-create

STATUS current

DESCRIPTION

"Spécifie la version de transfert TRAP qui est envoyée au système NMS considéré. Le réglage de cet objet à la valeur "disableSNMPv2trap(1)" provoque l'envoi du transfert en format SNMPv1 à un système NMS particulier. Le réglage de cet objet à la valeur "EnableSNMPv2trap(2)" provoque l'envoi du transfert en format SNMPv2 à un système NMS particulier."

DEFVAL { Disable SNMPv2trap }

::={docsDevNmAccessEntry 8}

Mode de coexistence utilisant la version SNMPv1/v2c/v3

En mode de coexistence utilisant la version SNMPv3, le service PS DOIT prendre en charge les règles spécifiées dans le § 11.3.3.1.2 concernant "l'initialisation SNMPv3" et les "modifications de clé DH". Ces règles comprennent le calcul des paramètres publics de la table de démarrage du modèle USM à codage Diffie-Helman (DH). Les règles suivantes s'appliquent au fonctionnement du service PS pendant et après le calcul des paramètres (valeurs) publics comme suit:

Pendant le calcul des valeurs publiques de la table usmDHKickstartTable:

- le service portail NE DOIT PAS permettre d'accès SNMP à partir du réseau WAN;
- le service portail PEUT continuer à permettre l'accès à partir du réseau LAN avec la limitation d'accès configurée par la base MIB de modèle USM, par la base MIB de communauté et par la base MIB de modèle VACM.

Après le calcul des valeurs publiques de la table usmDHKickstartTable:

- le service portail DOIT envoyer le transfert de démarrage à froid ou de démarrage à chaud afin d'indiquer que le service portail est maintenant pleinement compatible avec la version SNMPv3;
- les paquets SNMPv1/v2c/v3 sont traités comme décrit par les appels de commentaires RFC 2576, RFC 3412, RFC 3413, RFC 3414 et RFC 3415;
- la table docsDevNmAccessTable n'est pas accessible;
- les destinations de commande d'accès et de transfert sont déterminées par la table snmpCommunityTable, par la base MIB de notification, par la base MIB de cible, par la base MIB de modèle VACM et par la base MIB de modèle USM. Le service PS DOIT appliquer la politique d'accès de gestion définie par la vue de modèle VACM configurée par le câblo-opérateur, pour tout accès aux objets de base MIB spécifiés, sans considération de l'interface ou du protocole d'accès utilisé;
- la base MIB de communauté commande la conversion de la chaîne communautaire de paquet SNMPv1/v2c en nom de sécurité qui choisit les entrées dans la base MIB de modèle USM. La commande d'accès est fournie par la base MIB de modèle VACM;
- les bases MIB de modèle USM et de modèle VACM contrôlent les paquets SNMPv3;
- les destinations de transfert sont spécifiées dans les bases MIB de cible et de notification.

En cas d'échec de l'achèvement de l'initialisation SNMPv3 pour un utilisateur (c'est-à-dire que le système NMS ne peut pas accéder au service portail via l'unité PDU de la version SNMPv3), la table d'utilisateur de modèle USM DOIT être supprimée pour cet utilisateur, le service portail est en

mode de coexistence et le service portail ne permet l'accès en version SNMPv1/v2c que si et seulement si les entrées de base MIB de communauté (et les entrées qui s'y rapportent) sont configurées.

6.3.6.2 Mode de gestion de réseau pour un service PS fonctionnant en mode d'approvisionnement SNMP

Si le service PS fonctionne en mode d'approvisionnement SNMP après acquittement ACK en protocole DHCP (ce qui est indiqué par une valeur de '2' (SNMPmode) dans l'objet cabhPsDevProvMode), ce service passe en mode de coexistence SNMPv3 et utilise par défaut la version SNMPv3 afin d'échanger des messages de gestion avec le système NMS. Il utilise également le serveur Kerberos afin d'échanger des données de clé avec le centre KDC, conformément aux règles décrites dans le présent paragraphe.

6.3.6.2.1 Vues de gestion

Les commandes de gestion définies pour IPCable2Home résident dans la fonction de portail CMP du service portail. Les réglages, fondés sur le mode de gestion, définissent les droits d'accès qui sont attribués à un utilisateur pour l'accès à la base de données des services PS, par l'intermédiaire de bases MIB spécifiées par IPCable2Home, en protocole SNMP à partir du système NMS du réseau câblé. Un utilisateur unique est défini par la présente spécification IPCable2Home.

La Figure 6-4 illustre quelques exemples de vues de gestion possibles pour le service PS. Le modèle IPCable2Home définit une vue d'administrateur de réseau WAN (vue d'administrateur de services PS) et un utilisateur-administrateur de réseau WAN (utilisateur-administrateur de services PS). D'autres vues et utilisateurs, tels que la vue de maintenance de réseau WAN, la vue d'administrateur de réseau LAN, ou la vue d'utilisateur de réseau LAN peuvent être établis par l'autorité ultime (administrateur du service portail), selon les règles définies dans RFC 3414 et RFC 3415.

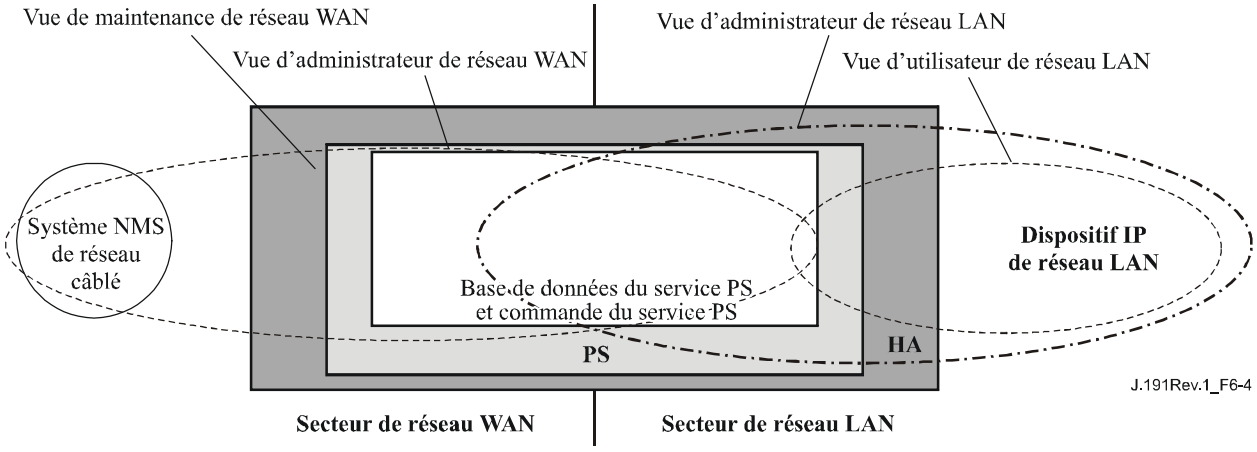


Figure 6-4/J.191 – Vues de gestion

Les paramètres gérés qui sont définis par IPCable2Home sont stockés dans la base de données du service portail. Comme indiqué dans la Figure 6-4, il y a une notion de vue d'accès à la base de données de services PS et à la commande de services PS qui permet la gestion simultanée à partir du réseau LAN comme du réseau WAN en définissant des vues de gestion dans la base de données PS et dans la commande PS. Ces vues sont un mécanisme permettant d'offrir la confidentialité et la sécurité. La politique correspondante peut être réglée séparément par l'utilisateur-administrateur du service PS.

L'autorité ultime (utilisateur-administrateur du service PS) possède ses propres identificateurs et clés d'utilisateur, avec les responsabilités suivantes:

- établissement de toutes les vues d'accès aussi bien à l'interface de gestion de réseau LAN qu'à l'interface de gestion de réseau WAN;
- création et gestion de tous les profils d'utilisateur, y compris les identificateurs d'utilisateur, les clés et les privilèges d'accès aux bases de données du service PS;
- établissement de la politique d'accès du côté LAN comme du côté WAN.

Une implémentation complète du modèle VACM exige un ensemble d'actions qui vont lier un "utilisateur" à un "groupe", et lier le "groupe" à une vue du modèle VACM, qui définit l'accès. Le § 6.3.6.3 décrit la façon de créer ces relations.

Le nom vacmSecurityName est "l'utilisateur". Ce nom de sécurité est lié au nom vacmGroupName et "l'utilisateur" est donc lié à un groupe spécifique qui est ensuite défini afin de spécifier quel niveau de sécurité est utilisé et aussi quelles vues de lecture, écriture et notification sont disponibles pour ce groupe. Les vues sont alors spécifiées afin de montrer exactement quels objets de base MIB sont accessibles.

Le modèle de commande fondé sur la vue détermine les droits d'accès d'un groupe, représentant zéro, un ou plusieurs noms de sécurité, qui ont les mêmes droits d'accès. Pour un contexte particulier, identifié par le nom de contexte (contextName), auquel un groupe identifié par le nom de groupe a accès en utilisant un modèle de sécurité et un niveau de sécurité particuliers, ces droits d'accès de groupe sont donnés par une vue de lecture, par une vue d'écriture et par une vue de notification.

La vue de lecture représente l'ensemble des instances d'objets autorisées pour le groupe lors de la lecture d'objets, laquelle intervient lors du traitement d'une opération d'extraction (lors du traitement d'unités PDU de la classe Lecture).

La vue d'écriture représente l'ensemble des instances d'objet autorisées pour le groupe lors de l'écriture d'objets, laquelle intervient lors du traitement d'une opération d'écriture (lors du traitement d'unités PDU de la classe Ecriture).

La vue de notification représente l'ensemble des instances d'objets autorisées pour le groupe lors de l'envoi d'objets dans une notification, comme lors de l'envoi d'une notification (lors de l'envoi d'unités PDU de la classe Notification).

La vue d'administrateur PS fournit un accès en lecture et en écriture complet à toutes les bases MIB spécifiées.

Les exigences relatives à la vue de gestion sont spécifiées au § 6.3.6.3.

6.3.6.2.2 Commande d'accès au réseau WAN

La commande d'accès SNMP, selon RFC 3415, sera utilisée afin de contrôler l'accès à des objets spécifiés de base MIB, sans considération de l'interface par laquelle la requête arrive. Le modèle de commande d'accès fondé sur la vue (VACM, *view-based access control model*) [RFC 3415] définit un ensemble de services qui peuvent être utilisés afin de vérifier les droits d'accès. Les groupes du modèle VACM définissent les droits d'accès au portail CMP.

Comme défini dans RFC 3415, section 2.4, une "vue de base MIB" est un ensemble spécifique de types d'objets gérés qui peuvent être définis. Dans le système IPCable2Home, cette notion sert à la prise en charge de la gestion de réseau WAN du service PS. L'accès et la vue d'utilisateur-administrateur du service PS sont spécifiés aux § 11.3.3.2.2 et 6.3.6.3. Le § 12.3.1 donne un exemple de séquence d'accès à une base de donnée de services PS à partir de l'interface avec le réseau WAN.

6.3.6.2.3 Sécurité

La sécurité des messages de gestion est assurée par le protocole SNMPv3. Voir au § 11 une description détaillée de la façon dont le protocole SNMPv3 est utilisé. Le portail CMP peut utiliser le protocole SNMPv3 afin de contrer les menaces identifiées à l'Annexe C.

Pour se protéger contre les attaques par réexécution, une horloge en temps réel sert à fournir des marqueurs temporels de messagerie. Les exigences de sécurité des messages de gestion sont spécifiées au § 11.3.3.

6.3.6.3 Exigences du modèle de commande d'accès fondée sur la vue (VACM)

Afin d'assurer le contrôle d'accès aux informations de gestion et de créer des secteurs de gestion distincts, le modèle de commande d'accès fondée sur la vue (VACM) DOIT être employé comme défini par RFC 3415.

'CHAdministrator' est le nom d'utilisateur du modèle USM [RFC 3414] défini aux § 6.3.4 et 6.3.6.2.1 du réseau WAN, qui est censé être le câblo-opérateur. Comme dans le cas de l'autorité ultime d'un service PS, l'administrateur de réseau WAN a besoin d'être en mesure de lire et d'écrire tout objet de base MIB ainsi que de créer de nouveaux utilisateurs. Les réglages de vue pour cet utilisateur 'CHAdministrator' sont définis dans le présent paragraphe.

La vue de l'administrateur WAN DOIT être implémentée dans un élément de services PS. Les vues par défaut autres que la vue d'administrateur WAN NE DOIVENT PAS être disponibles dans le service portail.

D'autres vues PEUVENT être créées par l'autorité ultime au moyen du système NMS du réseau câblé, par configuration de la base MIB du modèle VACM.

La spécification d'utilisateur concernant la vue d'administrateur WAN DOIT être implémentée comme suit:

vacmSecurityModel	3 (USM)
vacmSecurityName	"Administrateur du service PS"
vacmGroupName	"Administrateur du service PS"
vacmSecurityToGroupStorageType	permanent
vacmSecurityToGroupStatus	actif

La spécification de groupe pour la vue d'administrateur du service PS DOIT être implémentée comme suit:

PS Administrator Group	
vacmGroupName	"Administrateur du service PS"
vacmAccessContextPrefix	"
vacmAccessSecurityModel	3 (USM)
vacmAccessSecurityLevel	AuthPriv
vacmAccessContextMatch	exact
vacmAccessReadViewName	"Administrateur du service PS"
vacmAccessWriteViewName	"Administrateur du service PS"
vacmAccessNotifyViewName	"Administrateur du service PS"
vacmAccessStorageType	permanent
vacmAccessStatus	actif

La vue VACM pour la vue de l'administrateur du service PS DOIT être implémentée comme suit:

sous-arbre de vue d'administrateur du service PS 1.3.6.1 (base MIB entière)

6.3.6.4 Mappage des nuplets TLV dans les rangées de la table SNMPv3 créée

Le présent paragraphe ainsi que les paragraphes suivants décrivent en détail comment l'élément du fichier de configuration PS *docsisV3 Notification Receiver* (TLV de type 38) est mappé dans les tables fonctionnelles SNMPv3.

Dès réception d'un élément du fichier de configuration PS de type 38, le service PS DOIT introduire des entrées dans les tables suivantes de façon à provoquer la transmission du transfert correspondante:

- snmpNotifyTable;
- snmpTargetAddrTable;
- snmpTargetAddrExtTable;
- snmpTargetParamsTable;
- snmpNotifyFilterProfileTable;
- snmpNotifyFilterTable;
- snmpCommunityTable;
- usmUserTable;
- vacmSecurityToGroupTable;
- vacmAccessTable;
- vacmViewTreeFamilyTable.

Un fichier de configuration PS PEUT contenir des éléments TLV (de type 28) de base MIB qui créent des entrées dans l'une quelconque des 11 tables énumérées ci-dessus. Ces éléments TLV de base MIB sont censés ne pas comporter de colonnes d'indice commençant par les caractères "@config" ou "@PSconfig".

Les tables contenues dans le présent paragraphe montrent comment les champs extraits de l'élément TLV du fichier de configuration PS (les balises figurant entre chevrons <>) sont placés dans les tables SNMPv3.

La correspondance entre nuplets TLV et balises de table <TAG> est indiquée ci-dessous:

PS<Adresse IP> TLV 38.1

<Point d'accès> TLV 38.2

<Type de transfert> TLV 38.3

<Temporisation> TLV 38.4

<Réessais> TLV 38.5

<OID de filtre> TLV 38.6

<Nom de sécurité> TLV 38.7

Ces tables sont reproduites dans l'ordre où l'agent les explorera de haut en bas lorsqu'une notification sera produite afin de déterminer le destinataire de cette notification et la façon de remplir le paquet de notification.

6.3.6.4.1 snmpNotifyTable

Créer 2 rangées avec des valeurs fixes, si un ou plusieurs éléments TLV sont présents.

Tableau 6-4/J.191 – snmpNotifyTable

snmpNotifyTable [RFC 2573] SNMP-NOTIFICATION-MIB	Première rangée	Seconde rangée
Nom de colonne (* = Partie de l'indice)	Valeur de colonne	Valeur de colonne
* snmpNotifyName	"@PSconfig_inform"	"@PSconfig_trap"
snmpNotifyTag	"@PSconfig_inform"	"@PSconfig_trap"
snmpNotifyType	inform(2)	trap(1)
snmpNotifyStorageType	volatile	volatile
snmpNotifyRowStatus	Active(1)	Active(1)

6.3.6.4.2 snmpTargetAddrTable

Créer une seule rangée pour chaque élément TLV contenu dans le fichier de configuration.

Tableau 6-5/J.191 – snmpTargetAddrTable

snmpTargetAddrTable [RFC 2573] SNMP-TARGET-MIB	Nouvelle rangée
Nom de colonne (* = partie de l'indice)	Valeur de colonne
* snmpTargetAddrName	"@PSconfig_n", où n va de 0 à m – 1, et où m est le nombre d'éléments TLV du récepteur de notification contenus dans le fichier de configuration PS
snmpTargetAddrTDomain	snmpUDPDomain – snmpDomains.1
snmpTargetAddrTAddress (Adresse IP et Point d'accès du récepteur de notification)	OCTET STRING (6) Octets 1-4: <Adresse IP> Octets 5-6: <Point d'accès>
snmpTargetAddrTimeout	<Temporisation> d'après l'élément TLV
snmpTargetAddrRetryCount	<Réessais> d'après l'élément TLV
snmpTargetAddrTagList	Si <Type de transfert> == 1,2, ou 4 "@PSconfig_trap" Sinon si <Type de transfert> = 3 ou 5 "@PSconfig_inform"
snmpTargetAddrParams	"@PSconfig_n" (même valeur que la colonne snmpTargetAddrName)
snmpTargetAddrStorageType	volatile
snmpTargetAddrRowStatus	active(1)

6.3.6.4.3 snmpTargetAddrExtTable

Créer une seule rangée pour chaque élément TLV contenu dans le fichier de configuration.

Tableau 6-6/J.191 – snmpTargetAddrExtTable

snmpTargetAddrExtTable [RFC 2576] SNMP-COMMUNITY-MIB	**Nouvelle rangée**
Nom de colonne (* = partie de l'indice)	Valeur de colonne
* snmpTargetAddrExtName	"@PSconfig_n", où n va de 0 à m – 1, et où m est le nombre d'éléments TLV du récepteur de notification contenus dans le fichier de configuration PS
snmpTargetAddrMask	<chaîne d'octets de longueur égale à zéro>
snmpTargetAddrMMS	0

6.3.6.4.4 snmpTargetParamsTable

Créer 1 rangée pour chaque élément TLV contenu dans le fichier de configuration. Si <Type de transfert> est 1, 2, ou 3, ou si le champ <Nom de sécurité> a une longueur égale à zéro, créer la table comme suit:

Tableau 6-7/J.191 – snmpTargetParamsTable pour <Type de transfert> 1, 2, ou 3

snmpTargetParamsTable [RFC 2573] SNMP-TARGET-MIB	**Nouvelle rangée**
Nom de colonne (* = partie de l'indice)	Valeur de colonne
* snmpTargetParamsName	"@PSconfig_n", où n va de 0 à m – 1, et où m est le nombre d'éléments TLV du récepteur de notification contenus dans le fichier de configuration PS
snmpTargetParamsMPModel SYNTAX: SnmpMessageProcessingModel	Si <Type de transfert> = 1 SNMPv1(0) Sinon si <Type de transfert> = 2 ou 3 SNMPv2c(1) Sinon si <Type de transfert> = 4 ou 5 SNMPv3(3)
snmpTargetParamsSecurityModel SYNTAX: SnmpSecurityModel	Si <Type de transfert> = 1 SNMPv1(1) Sinon si <Type de transfert> = 2 ou 3 SNMPv2c(2) Sinon si <Type de transfert> = 4 ou 5 USM(3) NOTE – Le mappage des types du protocole SNMP vers une valeur est ici différent de la colonne snmpTargetParamsMPModel.
snmpTargetParamsSecurityName	"@PSconfig"
snmpTargetParamsSecurityLevel	noAuthNoPriv
snmpTargetParamsStorageType	volatile
snmpTargetParamsRowStatus	active(1)

Si <Type de transfert> est 4 ou 5, et le champ <Nom de sécurité> a une longueur différente de zéro, créer la table comme suit:

Tableau 6-8/J.191 – snmpTargetParamsTable pour <Type de transfert> 4 ou 5

snmpTargetParamsTable [RFC 2573] SNMP-TARGET-MIB	**Nouvelle rangée**
Nom de colonne (* = partie de l'indice)	Valeur de colonne
* snmpTargetParamsName	"@PSconfig_n", où n va de 0 à m – 1, et où m est le nombre d'éléments TLV du récepteur de notification contenus dans le fichier de configuration PS
snmpTargetParamsMPModel SYNTAX: SnmpMessageProcessingModel	Si <Type de transfert> = 1 SNMPv1(0) Sinon si <Type de transfert> = 2 ou 3 SNMPv2c(1) Sinon si <Type de transfert> = 4 ou 5 SNMPv3(3)
snmpTargetParamsSecurityModel SYNTAX: SnmpSecurityModel	Si <Type de transfert> = 1 SNMPv1(1) Sinon si <Type de transfert> = 2 ou 3 SNMPv2c(2) Sinon si <Type de transfert> = 4 ou 5 USM(3) NOTE – Le mappage des types du protocole SNMP vers une valeur est ici différent de la colonne snmpTargetParamsMPModel.
snmpTargetParamsSecurityName	<Nom de sécurité>
snmpTargetParamsSecurityLevel	Le niveau de sécurité du <Nom de sécurité>
snmpTargetParamsStorageType	volatile
snmpTargetParamsRowStatus	active(1)

6.3.6.4.5 snmpNotifyFilterProfileTable

Créer une seule rangée pour chaque TLV qui possède une <Longueur de filtre> différente de zéro.

Tableau 6-9/J.191 – snmpNotifyFilterProfileTable

snmpNotifyFilterProfileTable [RFC 2573] SNMP-NOTIFICATION-MIB	**Nouvelle rangée**
Nom de colonne (* = Partie de l'indice)	Valeur de colonne
* snmpTargetParamsName	"@PSconfig_n", où n va de 0 à m – 1 et où m est le nombre d'éléments TLV du récepteur de notification contenus dans le fichier de configuration PS.
snmpNotifyFilterProfileName	"@PSconfig_n", où n va de 0 à m – 1 et où m est le nombre d'éléments TLV du récepteur de notification contenus dans le fichier de configuration PS.
snmpNotifyFilterProfileStorType	volatile
snmpNotifyFilterProfileRowStatus	active(1)

6.3.6.4.6 snmpNotifyFilterTable

Créer une seule rangée pour chaque TLV qui possède une <Longueur de filtre> différente de zéro.

Tableau 6-10/J.191 – snmpNotifyFilterTable

snmpNotifyFilterTable [RFC 2573] SNMP-NOTIFICATION-MIB	Nouvelle rangée
Nom de colonne (* = Partie de l'indice)	Valeur de colonne
* snmpNotifyFilterProfileName	"@PSconfig_n" , où n va de 0 à m – 1 et où m est le nombre d'éléments TLV du récepteur de notification contenus dans le fichier de configuration PS.
* snmpNotifyFilterSubtree	<OID de filtre> d'après l'élément TLV
snmpNotifyFilterMask	<Chaîne d'octets de longueur égale à zéro>
snmpNotifyFilterType	inclus(1)
snmpNotifyFilterStorageType	volatile
snmpNotifyFilterRowStatus	active(1)

6.3.6.4.7 snmpCommunityTable

Créer une seule rangée avec des valeurs fixes si 1 ou plusieurs éléments TLV sont présents. Il en découle que les notifications selon les versions SNMPv1 et v2c contiennent la chaîne de communauté dans le nom snmpCommunityName.

Tableau 6-11/J.191 – snmpCommunityTable

snmpCommunityTable [RFC 2576] SNMP-COMMUNITY-MIB	Première rangée
Nom de colonne (* = Partie de l'indice)	Valeur de colonne
* snmpCommunityIndex	"@PSconfig"
snmpCommunityName	"public"
snmpCommunitySecurityName	"@PSconfig"
snmpCommunityContextEngineID	<The PS engineID>
snmpCommunityContextName	<Chaîne d'octets de longueur égale à zéro>
snmpCommunityTransportTag	<Chaîne d'octets de longueur égale à zéro>
snmpCommunityStorageType	volatile
snmpCommunityStatus	active(1)

6.3.6.4.8 usmUserTable

Créer une seule rangée avec des valeurs fixes, si un ou plusieurs éléments TLV sont présents. D'autres rangées sont créées chaque fois que l'identificateur d'automate d'un récepteur de transferts est découvert. Cette table spécifie le nom de l'utilisateur auquel les récepteurs de notification distants doivent envoyer les notifications.

Une seule rangée est créée dans la table usmUserTable. Puis, dès que l'identificateur d'automate de chaque récepteur de notification est découvert, l'agent copie cette rangée dans une nouvelle rangée et remplace la valeur 0x00 figurant dans la colonne usmUserEngineID par la valeur qui vient d'être découverte.

Tableau 6-12/J.191 – usmUserTable

usmUserTable [RFC 2574] SNMP-USER-BASED-SM-MIB	Première rangée
Nom de colonne (* = Partie de l'indice)	Valeur de colonne
* usmUserEngineID	0
* usmUserName	"@PSconfig" Lorsque d'autres rangées sont créées, celle-ci est remplacée par le champ <Nom de sécurité> d'après l'élément TLV.
usmUserSecurityName	"@PSconfig" Lorsque d'autres rangées sont créées, celle-ci est remplacée par le champ <Nom de sécurité> d'après l'élément TLV.
usmUserCloneFrom	<valeur indifférente> – cette rangée ne peut pas être clonée
usmUserAuthProtocol	Néant. Lorsque d'autres rangées sont créées, celle-ci est remplacée par Néant ou par MD5, selon le niveau de sécurité de l'utilisateur de la version v3.
usmUserAuthKeyChange	<valeur indifférente> – écriture seulement
usmUserOwnAuthKeyChange	<valeur indifférente> – écriture seulement
usmUserPrivProtocol	Néant. Lorsque d'autres rangées sont créées, celle-ci est remplacée par Néant ou par DES, selon le niveau de sécurité de l'utilisateur de la version v3.
usmUserPrivKeyChange	<valeur indifférente> – écriture seulement
usmUserOwnPrivKeyChange	<valeur indifférente> – écriture seulement
usmUserPublic	<chaîne de longueur égale à zéro>
usmUserStorageType	volatile
usmUserStatus	active(1)

6.3.6.4.9 vacmSecurityToGroupTable

Créer trois rangées avec des valeurs fixes, si un ou plusieurs éléments TLV sont présents.

Il s'agit des trois rangées ayant des valeurs fixes. Elles sont utilisées pour les entrées d'élément TLV dont le <Type de transfert> est réglé à 1, 2, ou 3 ou dont le champ <Nom de sécurité> a une longueur égale à zéro.

Tableau 6-13/J.191 – vacmSecurityToGroupTable

vacmSecurityToGroupTable [RFC 2575] SNMP-VIEW-BASED-ACM-MIB	Première rangée	Seconde rangée	Troisième rangée
Nom de colonne (* = Partie de l'indice)	Valeur de colonne	Valeur de colonne	Valeur de colonne
* vacmSecurityModel	SNMPv1(1)	SNMPv2c(2)	USM(3)
* vacmSecurityName	"@PSconfig"	"@PSconfig"	"@PSconfig"
vacmGroupName	"@PSconfigv1"	"@PSconfigv2"	"@PSconfigUSM"
vacmSecurityToGroupStorageType	volatile	volatile	volatile
vacmSecurityToGroupStatus	active(1)	active(1)	active(1)

6.3.6.4.10 vacmAccessTable

Créer trois rangées avec des valeurs fixes, si un ou plusieurs éléments TLV sont présents.

Il s'agit des trois rangées ayant des valeurs fixes. Elles sont utilisées pour les entrées d'élément TLV dont le <Type de transfert> est réglé à 1, 2, ou 3 ou dont le champ <Nom de sécurité> a une longueur égale à zéro.

Tableau 6-14/J.191 – vacmAccessTable

vacmAccessTable [RFC 2575] SNMP-VIEW-BASED-ACM-MIB	Première rangée	Seconde rangée	Troisième rangée
Nom de colonne (* = Partie de l'indice)	Valeur de colonne	Valeur de colonne	Valeur de colonne
* vacmGroupName	"@PSconfigV1"	"@PSconfigV2"	"@PSconfigUSM"
* vacmAccessContextPrefix	<Chaîne de longueur égale à zéro>	<Chaîne de longueur égale à zéro>	<Chaîne de longueur égale à zéro>
* vacmAccessSecurityModel	SNMPv1(1)	SNMPv2c(2)	USM(3)
* vacmAccessSecurityLevel	noAuthNoPriv(1)	noAuthNoPriv(1)	noAuthNoPriv(1)
vacmAccessContextMatch	exact(1)	exact(1)	exact(1)
vacmAccessReadViewName	<Chaîne d'octets de longueur égale à zéro>	<Chaîne d'octets de longueur égale à zéro>	<Chaîne d'octets de longueur égale à zéro>
vacmAccessWriteViewName	<Chaîne d'octets de longueur égale à zéro>	<Chaîne d'octets de longueur égale à zéro>	<Chaîne d'octets de longueur égale à zéro>
vacmAccessNotifyViewName	"@PSconfig"	"@PSconfig"	"@PSconfig"
vacmAccessStorageType	volatile	volatile	volatile
vacmAccessStatus	active(1)	active(1)	active(1)

Les entrées d'élément TLV dont le <Type de transfert> est réglé à 4 ou 5 et possède un champ <Nom de sécurité> de longueur différente de zéro utiliseront les rangées créées dans la table vacmAccessTable par le processus de démarrage DH (Diffie-Helman).

6.3.6.4.11 vacmViewTreeFamilyTable

Créer une seule rangée avec des valeurs fixes si un ou plusieurs éléments TLV sont présents.

Cette rangée est utilisée pour les entrées d'élément TLV dont le <Type de transfert> est réglé à 1, 2, ou 3 ou dont le champ <Nom de sécurité> a une longueur égale à zéro.

Tableau 6-15/J.191 – vacmViewTreeFamilyTable

vacmViewTreeFamilyTable [RFC 2575] SNMP-VIEW-BASED-ACM-MIB	Première rangée
Nom de colonne (* = Partie de l'indice)	Valeur de colonne
* vacmViewTreeFamilyViewName	"@PSconfig"
* vacmViewTreeFamilySubtree	1.3
vacmViewTreeFamilyMask	<Valeur par défaut extraite de la base MIB>
vacmViewTreeFamilyType	incluse (1)
vacmViewTreeFamilyStorageType	volatile
vacmViewTreeFamilyStatus	active (1)

Les entrées d'élément TLV dont le champ <Type de transfert> est réglé à 4 ou 5 et dont le champ <Nom de sécurité> a une longueur différente de zéro utiliseront les rangées créées dans la table vacmViewTreeFamilyTable par le processus de démarrage DH (Diffie-Helman).

6.3.7 Exigences relatives à la base MIB

Les objets de base MIB dont la liste figure à l'Annexe A DOIVENT être implémentés dans un élément de services PS. Les objets de base MIB requis viennent des documents de base MIB suivants:

1) Base MIB de groupe d'interfaces [RFC 2863];
2) Base MIB de dispositif DOCSIS par câble [RFC 2669];
3) Base MIB de définition [E.4];
4) Base MIB de dispositif PSDev par câble [E.1];
5) Base MIB de portail CAP par câble [E.6];
6) Base MIB de portail CDP par câble [E.5];
7) Base MIB de portail CTP par câble [E.2];
8) Base MIB de sécurité par câble [E.3];
9) Fichier draft-ietf-ipcdn-bpiplus-mib-12;
10) Base MIB d'adresses IP (SNMPv2) [RFC 2011];
11) Base MIB de protocole UDP (SNMPv2) [RFC 2013];
12) Clé de modèle USM à codage Diffie-Helman [RFC 2786];
13) Base MIB d'adresses de réseau INET [RFC 3291];
14) Base MIB pour interfaces DOCSIS [RFC 2670];
15) Base MIB de types d'interface de l'autorité IANA.

Dans le service PS imbriqué, l'entité de gestion du CM et l'entité de gestion du PS (portail CMP) DOIVENT répondre à des adresses IP de gestion différentes et indépendantes. Le système de câblo-modem et le système IPCable2Home spécifient certains objets de base MIB qui leur sont communs mais, si un câblo-modem conforme et un élément PS conforme à IPCable2Home sont intégrés dans le même dispositif, chacun est tenu de conserver sa propre instance distincte des objets MIB spécifiés, accessibles au moyen de différentes adresses IP de gestion, à l'exception de la sous-arborescence snmpv2 selon RFC 2578, du groupe SNMP selon RFC 3418, des compteurs de groupe IP et ICMP selon RFC 2011, et des compteurs de groupe UDP selon RFC 2013, qui PEUVENT être communs et partagés entre le câblo-modem et l'élément de services PS, et qui PEUVENT être accessibles au moyen des adresses IP de gestion de câblo-modem ou des adresses IP de gestion du service PS.

Dans le service PS imbriqué, c'est le câblo-modem qui commande le téléchargement de logiciel de l'image unique des logiciels combinés de câblo-modem et de services PS. Le groupe d'objets docsDevSoftware [RFC 2669] NE DOIT PAS être implémenté dans le service PS imbriqué, à l'exception de l'objet docsDevSwCurrentVers en lecture seule, c'est-à-dire que le reste du groupe d'objets ci-après n'est accessible qu'au moyen de l'adresse IP de gestion du câblo-modem:

- docsDevSwServer;
- docsDevSwFilename;
- docsDevSwAdminStatus;
- docsDevSwOperStatus.

Le groupe d'objets docsDevSoftware DOIT être implémenté dans un service PS autonome. La modification des objets du groupe docsDevSoftware (comme spécifié au § 11.3.7) par le câblo-opérateur en vue du téléchargement de l'image logicielle du service PS autonome DOIT se traduire par une opération correcte et sécurisée de téléchargement de logiciel.

Dans le service PS imbriqué, les objets de base MIB de câblo-modem ne sont visibles et accessibles que lorsque le gestionnaire y accède au moyen de l'adresse IP de gestion du câblo-modem. Ils NE DOIVENT PAS être visibles ou accessibles au moyen d'une quelconque adresse IP de services PS, à l'exception de la sous-arborescence snmpv2 selon RFC 2578, du groupe SNMP selon RFC 3418, des compteurs de groupe IP et ICMP selon RFC 2011, et des compteurs de groupe UDP selon RFC 2013, qui sont autorisés à être partagés entre les entités de gestion CM et PS.

Dans le service PS imbriqué, les objets de base MIB spécifiés par IPCable2Home DOIVENT n'être visibles et accessibles que lorsque le gestionnaire y accède à partir du réseau WAN au moyen de l'adresse IP de réseau WAN-Man du service PS ou y accède à partir du réseau LAN au moyen de l'adresse IP du routeur cabhCdpServerRouter et ces objets NE DOIVENT PAS être visibles ou accessibles au moyen de l'adresse IP de gestion du câblo-modem, à l'exception de la sous-arborescence snmpv2 selon RFC 2578, du groupe SNMP selon RFC 3418, des compteurs de groupe IP et ICMP selon RFC 2011, et des compteurs de groupe UDP selon RFC 2013, qui sont autorisés à être partagés entre les entités de gestion CM et PS.

La hiérarchie générale des bases MIB est illustrée à la Figure 6-5. La liste des identificateurs OID spécifiquement nécessaires pour les bases MIB individuelles figure à l'Annexe A.

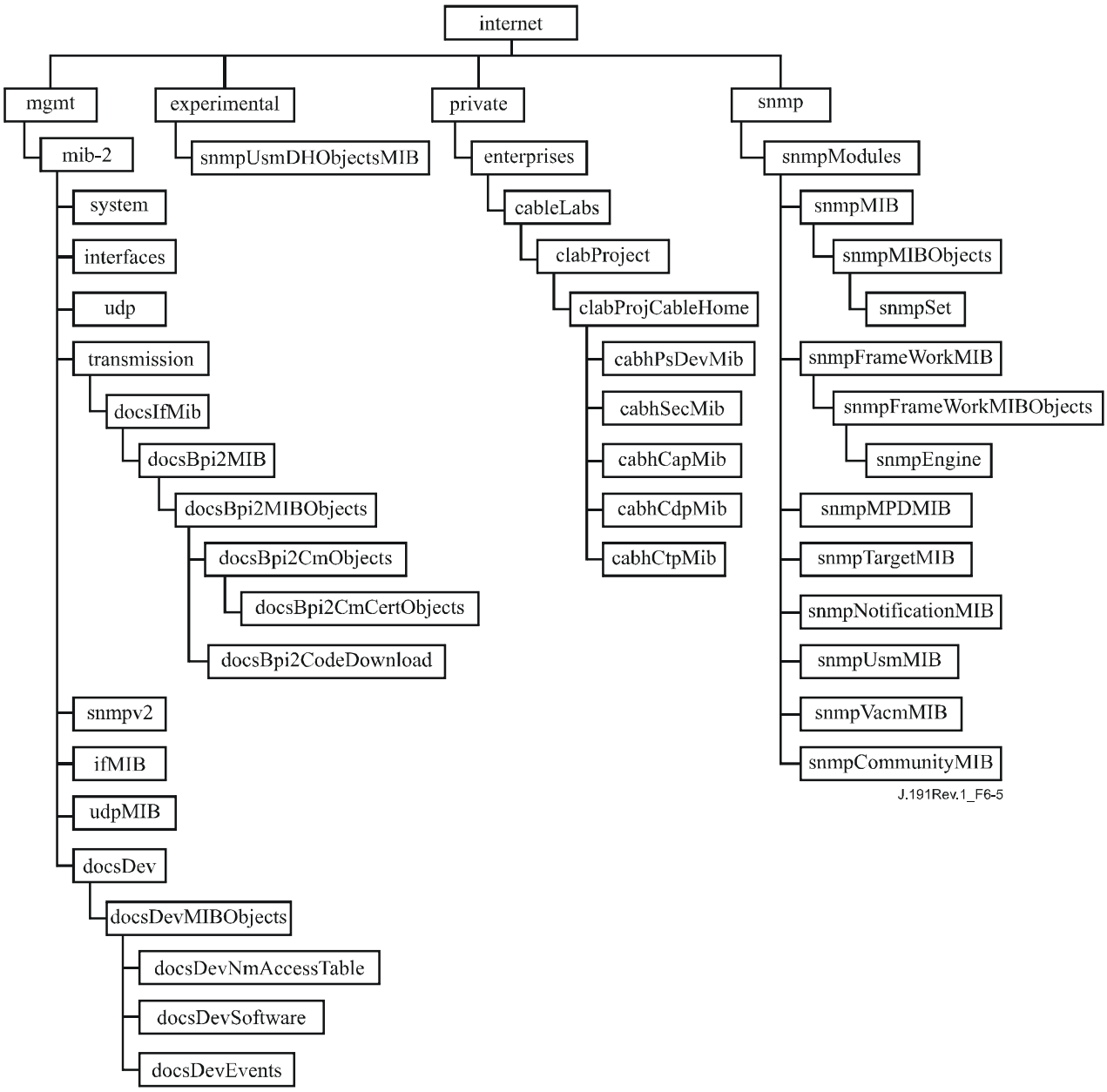


Figure 6-5/J.191 – Hiérarchie des bases MIB

6.3.8 Exigences relatives à la base MIB de groupe d'interfaces

La base MIB de groupe d'interfaces fournit un outil puissant afin de permettre aux câblo-opérateurs de comprendre l'état et de voir les statistiques de toutes les interfaces physiques avec l'élément de services PS. Afin de permettre une utilisation intelligente de cette base MIB, un système de numérotation des interfaces est essentiel. Il est donc nécessaire que les éléments de services portail se conforment aux exigences suivantes:

Une instance de l'entrée ifEntry DOIT exister pour l'interface WAN-MAN de l'élément de services PS, même si l'interface est interne – comme cela se produit dans le cas d'un service portail imbriqué utilisant une solution à microcircuit intégré.

Une instance de l'entrée ifEntry DOIT exister pour l'interface WAN-Data de l'élément de services PS, du moment que l'interface – qu'elle soit externe ou interne – fait partie de la configuration active du service PS, comme c'est le cas d'un service PS imbriqué utilisant une solution à microcircuit intégré.

Une instance de l'entrée IfEntry DOIT exister pour chaque interface LAN physique de l'élément de services PS. Une instance de l'entrée ifEntry DOIT exister pour une interface du groupe des 'interfaces LAN du côté des signaux résultants', qui est identifiée par la valeur d'indice ifIndex 255.

Les interfaces DOIVENT être numérotées comme indiqué au Tableau 6-16.

Tableau 6-16/J.191 – Numérotage des interfaces dans la table ifTable

Interface	Description
1	Interface WAN-MAN
2	Interface WAN-Data
2 + n	Chaque interface LAN
255	Interface LAN côté résultant

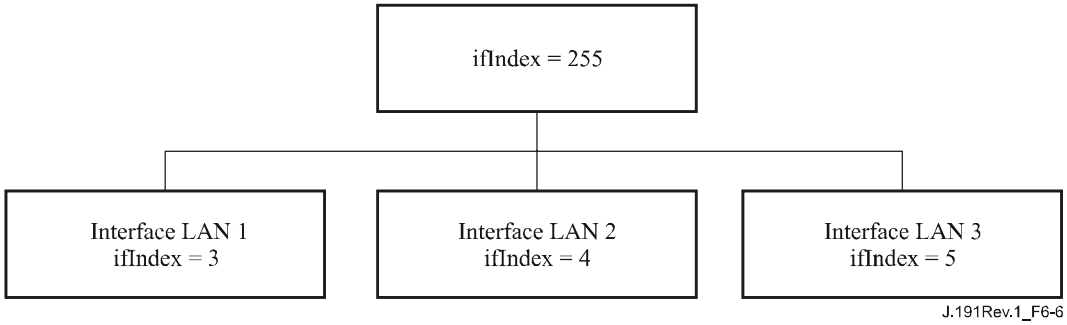
Si le statut ifAdminStatus d'une interface donnée a la valeur "down", cette interface NE DOIT PAS accepter ou réexpédier un quelconque trafic. L'objet ifAdminStatus correspondant à la valeur 255 de l'indice d'interface DOIT assurer la commande administrative de toutes les interfaces LAN et DOIT être implémenté en lecture-écriture.

Les valeurs de type d'interface (ifType) de la table ifTable correspondant à la valeur d'indice ifIndex 255 DOIVENT être "Other" (autre type). Dans le cas des services PS imbriqués, les valeurs de type d'interface (ifType) de la table ifTable correspondant aux valeurs d'indice ifIndex 1 et 2 DOIVENT être la valeur de type d'interface appropriée de l'autorité IANA.

La valeur d'adresse physique d'interface (ifPhysAddress) de la table ifTable correspondant à la valeur d'indice ifIndex 255 DOIT être une chaîne d'octets de longueur égale à zéro.

Les compteurs d'interfaces WAN ayant les valeur d'indice ifIndex 1 et 2 dans la table ifTable DOIVENT être partagés entre les deux interfaces. Les compteurs ifTable pour la valeur d'indice 255 PEUVENT être implémentés.

Le groupe ifStack DOIT être implémenté afin d'identifier les relations entre l'interface de couche supérieure du groupe des 'interfaces LAN du côté résultant' et les sous-interfaces LAN de couche inférieure. La Figure 6-6 décrit l'emploi du groupe ifStack pour un service PS à trois interfaces LAN.



Implémentation du groupe ifStack dans cet exemple:

Groupe ifStack de couche supérieure	Groupe ifStack de couche inférieure
255	3
255	4
255	5

Figure 6-6/J.191 – Exemple d'implémentation du groupe ifStack

6.3.9 Exigences relatives à la table ipNetToMediaTable

La table ipNetToMediaTable (RFC 2011) mappe des adresses IP sur des adresses physiques. Son emploi est clair si chaque adresse IP est associée à une seule interface physique et si chaque interface physique est associée à une seule adresse physique. Le service PS implémente cependant différentes adresses IP qui peuvent s'appliquer à plusieurs interfaces physiques. Il associe également l'interface physique avec le réseau WAN à deux adresses de matériel. Le service PS DOIT énumérer, dans la table ipNetToMediaTable, chacune des adresses IP qui font partie de sa configuration active, en créant une seule entrée par valeur IP distincte[1] et en appliquant la table suivante.

Tableau 6-17/J.191 – ipNetToMediaTable

Adresse ipNetToMediaNetAddress	Adresse ipNetToMediaPhysAddress	Indice ipNetToMediaIfIndex
Adresse IP de réseau WAN-Man	Adresse matérielle de réseau Wan-Man	1
Adresses IP de réseau WAN-Data	Adresse matérielle de réseau Wan-Data	2
Adresse IP de serveur DHCP	Chaîne d'octets de longueur égale à zéro	255
Adresse IP de serveur DNS	Chaîne d'octets de longueur égale à zéro	255
Adresse IP de routeur-serveur	Chaîne d'octets de longueur égale à zéro	255

6.4 Le portail d'essai du câble (CTP, *cable test portal*)

6.4.1 Objectifs du portail CTP

Les objectifs du portail d'essai du câble sont les suivants:

- permettre les diagnostics de dérangement de dispositif IP de réseau LAN;
- permettre la visibilité sur les dispositifs IP de réseau LAN, ainsi que l'accès aux numéros et aux types de dispositif IP de réseau LAN;
- permettre la surveillance de la performance du dispositif IP de réseau LAN.

6.4.2 Directives pour la conception du portail CTP

Les directives de conception du système d'utilitaires de gestion IPCable2Home sont énumérées dans le Tableau 6-18. Un certain nombre de ces directives reprennent les directives de conception du portail CMP, qui donnaient des indications pour la spécification des fonctionnalités du portail CTP.

[1] Pour chacune des adresses IP de serveur DHCP, de serveur DNS et de routeur-serveur, une seule entrée ne sera créée que si ces trois adresses sont distinctes. Dans la configuration la plus typique d'un réseau LAN de services PS, dans laquelle la même adresse IP est partagée par les trois serveurs, une seule entrée sera affichée dans la table ipNetToMediaTable.

Tableau 6-18/J.191 – Directives pour la conception du système de portail CMP

Référence	Directives pour la conception du système de portail CMP
CTP 1	Il est nécessaire que les interfaces acceptent les caractéristiques de gestion et de diagnostic et les fonctions requises pour la prise en charge des services câblés fournis dans le réseau du domicile.
CTP 2	Il est nécessaire que des capacités de surveillance locales et à distance permettent de surveiller le fonctionnement du réseau du domicile et aident le consommateur et le câblo-opérateur à identifier les zones de problème.
CTP 3	Le système NMS de réseau câblé exige une méthode pour rassembler les informations d'identification sur chaque dispositif IP connecté au réseau du domicile.
CTP 4	Le système NMS de réseau câblé exige une méthode pour détecter si un dispositif connecté est en état de fonctionnement.

6.4.3 Description du système de portail CTP

Le portail CTP (portail d'essai du câble) contient les "utilitaires distants" avec lesquels la gestion de système NMS peut collecter d'autres informations de dispositif LAN. Les essais doivent être effectués à distance, car contourner une fonction de traduction d'adresse de réseau (NAT, *network address translation*) dans un routeur risque d'être très difficile. Par exemple, une validation par écho de réseau WAN à réseau LAN ne pourra pas passer à travers un service PS, à moins que le portail CAP n'ait été préconfiguré pour laisser passer ce trafic. Le portail CTP est un mandataire local qui sert à interpréter et à exécuter la classe de dérangements/diagnostics à distance des messages SNMP qu'il reçoit de l'opérateur de système NMS. Ces essais de dispositif IP de réseau LAN sont définis sur la base des problèmes qu'on peut vraisemblablement rencontrer: diagnostics de connexité et de débit utile.

Ces fonctions sont appelées *utilitaire de vitesse de connexion de portail CTP* et *utilitaire de validation par écho de portail CTP*. Les utilitaires de vitesse de connexion et de validation par écho permettent au centre de prise en charge des consommateurs du câblo-opérateur et au centre d'exploitation du réseau d'en savoir plus sur la connexion entre l'élément de services PS et les dispositifs IP de réseau LAN chez l'utilisateur.

6.4.3.1 Utilitaire de vitesse de connexion de portail CTP

Cette fonction sert à obtenir une mesure grossière de la performance en termes de débit utile dans la liaison entre le service portail et le dispositif IP de réseau LAN. Elle envoie une rafale de paquets entre le service portail et le dispositif IP de réseau LAN soumis à l'essai, et le temps d'aller-retour est mesuré pour la rafale. En général, l'opérateur de système NMS introduit quelques paramètres et déclenche la fonction, dont les résultats sont mémorisés dans la base de données du service portail pour récupération ultérieure au moyen de la base MIB du portail CTP.

La fonction de vitesse de connexion repose sur l'incorporation d'une fonction de "bouclage" ou de "service d'écho" dans les dispositifs IP de réseau LAN. L'autorité chargée de l'assignation des numéros Internet (IANA, *Internet assigned numbers authority*) a attribué le point d'accès 7 de service d'écho à la fois au protocole TCP et au protocole UDP [RFC 347]. La valeur par défaut de l'adresse IP de la source (objet cabhCtpConnSrcIp) est la même que celle de la passerelle par défaut du réseau LAN du service PS (objet cabhCdpServerRouter). La valeur de l'adresse cabhCtpConnSrcIp peut être réglée à toute adresse IP valide de réseau WAN-Data du service PS ou à toute adresse IP valide d'interface LAN du service PS. L'adresse IP de réseau WAN-Man de PS n'est pas utilisée en tant qu'adresse IP de source pour un utilitaire de portail CTP car, lorsqu'une adresse IP de réseau WAN-Man de PS est présente mais qu'une adresse IP de réseau WAN-Data ne l'est pas, le service PS fonctionne en mode de traitement primaire de paquet par traversée et le câblo-opérateur peut au besoin essayer directement des dispositifs IP de réseau LAN à partir de la console du système NMS. Cette méthode d'essai ne fonctionne que sur des dispositifs IP de réseau

LAN se trouvant dans le secteur d'adresses de réseau LAN-Trans et implémentant la fonction de service d'écho décrite dans RFC 347.

Le paragraphe ci-dessous sur les exigences contrôlables du portail CTP énumère les paramètres et les réponses concernant l'utilitaire de vitesse de connexion. Le § 12.2.1.1 précise le fonctionnement de l'utilitaire de vitesse de connexion.

6.4.3.2 Utilitaire de validation par écho de portail CTP

On se sert de cette fonction pour contrôler la connexité entre le service portail et des dispositifs IP de réseau LAN individuels. Les résultats de multiples exécutions de l'essai par utilitaire de validation par écho peuvent être rassemblés par le système NMS afin de créer une exploration par le réseau des dispositifs IP de réseau LAN. La table DHCP du portail CDP contient un historique des dispositifs, mais seulement de ceux qui emploient le protocole DHCP. La validation par écho peut saisir un état actuel qui inclut des clients non DHCP. Pour garder une certaine simplicité au service portail, on suppose que le système NMS incrémente l'adresse et mémorise les résultats dans l'utilitaire NMS pour effectuer une exploration d'un sous-réseau LAN.

L'utilitaire de validation par écho (PING) est initialisé par une série de messages de demande d'établissement par protocole SNMP, produits par la console du système NMS du réseau câblé vers l'adresse de gestion du service portail.

L'utilitaire de validation par écho du portail CTP DOIT être implémenté au moyen de la fonction "écho" du protocole de message de commande Internet (ICMP, *Internet control message protocol*). Le portail CTP produira une demande d'écho ICMP et le dispositif IP de réseau LAN est censé renvoyer une réponse d'écho ICMP.

Le portail CTP DOIT ignorer et exclure du décompte cabhCtpPingNumRecv toute réponse en écho reçue après l'expiration de la temporisation cabhCtpPingTimeOut.

Le § 6.4.4 énumère les paramètres et réponses pour l'utilitaire de validation par écho.

Le § 12.2.1.2 détaille le fonctionnement de l'utilitaire de validation par écho.

6.4.4 Exigences relatives au portail CTP

6.4.4.1 Utilitaire de vitesse de connexion

Le portail CTP DOIT implémenter l'utilitaire de vitesse de connexion ET DOIT se conformer aux valeurs et aux étendues de valeurs qui ont été définies pour les objets propres à l'utilitaire de vitesse de connexion, contenus dans la base MIB de portail CTP par câble.

Le portail CTP DOIT transmettre les octets des données d'essai aussi rapidement que possible lors de l'application de l'utilitaire de vitesse de connexion.

Le portail CTP DOIT utiliser le point d'accès 7 comme point de destination lors de l'exécution de l'utilitaire de vitesse de connexion.

L'utilitaire de vitesse de connexion NE DOIT PAS produire de paquets à la sortie d'une quelconque interface avec le réseau WAN.

Lorsque le système NMS déclenche le lancement de l'utilitaire de vitesse de connexion par le portail CTP en réglant l'objet cabhConnControl à la valeur = start(1), le portail CTP DOIT effectuer les opérations suivantes:

- réinitialiser le temporisateur;
- régler l'objet cabhCtpConnStatus à la valeur = running(2);
- transmettre un nombre de paquets égal à la valeur du champ cabhCtpConnNumPkts, chaque paquet ayant une longueur égale à la valeur du champ cabhCtpConnPktSize, vers

l'adresse IP dont la valeur est celle du champ cabhCtpConnDestIp et dont le numéro de point d'accès est 7, au moyen du protocole spécifié par l'objet cabhCtpConnProto;

- armer le temporisateur avec le premier bit transmis;
- fermer le temporisateur lorsque le dernier bit est reçu en retour du dispositif IP de réseau LAN cible OU lorsque la valeur du temporisateur est égale à celle du champ cabhCtpConnTimeOut, selon celle qui arrive en premier;
- lorsque le temporisateur est fermé, régler l'objet cabhCtpConnStatus à la valeur = complete(3) ET signaler l'événement approprié (voir l'Annexe B – Evénements de portail CTP);
- mémoriser dans l'objet cabhCtpConnRTT la valeur (en millisecondes) du temporisateur;
- si la valeur du temporisateur est égale à celle du champ cabhCtpConnTimeOut avant que le dernier bit ait été reçu du dispositif IP de réseau LAN cible, signaler l'événement approprié (voir l'Annexe B – Evénements de portail CTP);
- calculer le débit utile comme défini dans la prescription ci-dessous et mémoriser la valeur dans l'objet cabhCtpConnThroughput.

Si l'utilitaire de vitesse de connexion est arrêté par le système NMS au moyen du réglage de l'objet cabhCtpConnControl à la valeur = abort(2) ou pour toute autre raison avant réception du dernier bit en provenance du dispositif IP de réseau LAN cible OU avant expiration du temporisateur, le portail CTP DOIT régler l'objet cabhCtpConnStatus à la valeur = aborted(4) ET signaler l'événement approprié (voir l'Annexe B – Evénements de portail CTP).

Lorsque le portail CTP exécute l'utilitaire de vitesse de connexion, il DOIT déterminer la valeur moyenne – en kilobits par seconde – du débit utile dans l'aller-retour entre le service PS et le dispositif IP de réseau LAN dont l'adresse est transmise par l'objet cabhCtpConnDestIp (c'est-à-dire le dispositif IP de réseau LAN cible), puis arrondir ce nombre au plus proche entier ET mémoriser ce résultat dans l'objet cabhCtpConnThroughput.

La charge utile des paquets transmis pendant l'exécution de l'utilitaire de vitesse de connexion NE DEVRAIT PAS être constituée uniquement de zéros ou de uns.

Le portail CTP DOIT réinitialiser à une valeur de 0 chacun des objets cabhCtpConnPktsSent, cabhCtpConnPktsRecv, cabhCtpConnRTT et cabhCtpConnThroughput, lorsque l'utilitaire de vitesse de connexion est lancé (c'est-à-dire lorsque la valeur de l'objet cabhCtpConnControl est mise à start(1)).

Le temps RTT de l'utilitaire de vitesse de connexion est mesuré dans le service PS en tant que durée écoulée entre le premier bit du premier paquet envoyé et le dernier bit du dernier paquet reçu. Le temps RTT n'est valide que si le nombre de paquets reçus est égal au nombre de paquets émis.

Le portail CTP DOIT autoriser le réglage de l'adresse IP de destination de l'utilitaire de vitesse de connexion (objet cabhCtpConnDestIp) à toute adresse IPv4 valide de tout dispositif IP de réseau LAN accessible au moyen de toute interface LAN du PS exécutant l'utilitaire de vitesse de connexion par portail CTP.

Le réglage à la valeur start(1) de l'objet de commande de l'utilitaire de vitesse de connexion – cabhCtpConnControl – DOIT provoquer l'exécution de l'utilitaire de vitesse de connexion.

Le réglage à la valeur abort(2) de l'objet de commande de l'utilitaire de vitesse de connexion – cabhCtpConnControl – DOIT provoquer la fin de l'exécution de l'utilitaire de vitesse de connexion.

La valeur par défaut de l'objet cabhCtpConnStatus est notRun(1), qui indique que l'utilitaire de vitesse de connexion n'a jamais été exécuté.

Le portail CTP DOIT régler à running(2) la valeur de l'objet cabhCtpConnStatus si l'utilitaire a été chargé de démarrer, ou n'a pas été terminé, ou si le temporisateur de vitesse de connexion n'est pas arrivé à expiration.

Le portail CTP DOIT régler à complete(3) la valeur de l'objet cabhCtpConnStatus lorsque le dernier paquet envoyé par l'utilitaire de vitesse de connexion est reçu par le portail CTP.

Le portail CTP DOIT régler à aborted(4) la valeur de l'objet cabhCtpConnStatus si, après avoir été lancé, l'utilitaire de vitesse de connexion est terminé par un réglage SNMP de l'objet cabhCtpConnControl à la valeur abort(2) ou si l'essai est terminé autrement avant que le dernier paquet envoyé par l'utilitaire de vitesse de connexion ait été reçu ET avant que le temporisateur de l'utilitaire de vitesse de connexion (objet cabhCtpConnTimeOut) soit arrivé à expiration.

Le portail CTP DOIT régler à timeOut(5) la valeur de l'objet cabhCtpConnStatus si le temporisateur de l'utilitaire de vitesse de connexion (objet cabhCtpConnTimeOut) arrive à expiration avant que le dernier paquet envoyé par l'utilitaire de vitesse de connexion ait été reçu par le portail CTP.

Le portail CTP NE DOIT PAS utiliser une quelconque adresse IP comme adresse IP de source de l'utilitaire de vitesse de connexion (objet cabhCtpConnSrcIp) à l'exception d'une adresse IP actuelle et valide du réseau WAN-Data du PS (c'est-à-dire une valeur active de l'objet cabhCdpWanDataAddrIp) OU une adresse IP actuelle et valide de l'interface avec le réseau LAN du PS. Si une valeur non valide est configurée pour l'objet cabhCtpConnSrcIp, le portail CTP DOIT traiter l'exécution de l'essai comme un cas abandonné et régler à la valeur 'aborted' l'objet cabhCtpConnStatus indiquant le statut de l'utilitaire de vitesse de connexion puis signaler l'événement approprié (voir le Tableau B.1).

6.4.4.2 Utilitaire de validation par écho

Le portail CTP DOIT implémenter l'utilitaire de validation par écho du portail CTP ET DOIT se conformer aux valeurs et étendues de valeurs par défaut qui ont été définies pour les objets propres à l'utilitaire de validation par écho de la base MIB de portail CTP par câble.

Lorsque le système NMS déclenche le lancement de l'utilitaire de validation par écho par le portail CTP en réglant l'objet cabhCtpPingControl à la valeur = start(1), le portail CTP DOIT effectuer les opérations suivantes:

- régler l'objet cabhCtpPingStatus à la valeur = running(2);
- envoyer à l'adresse IP définie par la valeur de l'objet cabhCtpPingDestIp autant de validations par écho (requêtes ICMP) que spécifié par la valeur de l'objet cabhCtpPingNumPkts, en utilisant comme adresse de source de chaque requête la valeur de l'objet cabhCtpPingSrcIp. La longueur de chaque trame d'essai est la valeur de l'objet cabhCtpPingPktSize. La temporisation de chaque validation est la valeur de l'objet cabhCtpPingTimeOut;
- attendre pendant la durée définie par la valeur de l'objet cabhCtpPingTimeBetween entre chaque demande de validation émise par le portail CTP si la valeur de l'objet cabhCtpPingNumPkts est supérieure à 1.

Si le portail CTP reçoit toutes les réponses de validation par écho avant l'expiration d'un quelconque temporisateur, ce portail CTP DOIT régler l'objet cabhCtpPingStatus à la valeur = complete(3) ET signaler l'événement approprié (voir Annexe B – Evénements de portail CTP).

Si le système NMS met fin à l'utilitaire de validation par écho en réglant l'objet cabhCtpPingControl à la valeur = abort(2) ou pour toute autre raison avant que le dernier bit soit reçu du dispositif IP de réseau LAN cible ET avant que la temporisation ait expiré, le portail CTP DOIT régler l'objet cabhCtpPingStatus à la valeur =aborted(4) ET signaler l'événement approprié (voir Annexe B – Evénement de portail CP).

Si le temporisateur arrive à expiration au cours d'au moins une des validations par écho, avant que sa réponse soit reçue du dispositif IP de réseau LAN cible, le portail CTP DOIT régler l'objet cabhCtpPingStatus à la valeur = timedOut(5) ET signaler l'événement approprié (voir Annexe B – Evénements de portail CTP).

Lorsqu'il exécute l'utilitaire de validation par écho, le portail CTP DOIT déterminer le temps d'aller-retour moyen entre le service PS et le dispositif IP de réseau LAN dont l'adresse est communiquée par l'objet cabhCtpPingDestIp (le dispositif IP de réseau LAN cible), calculé sur le nombre de requêtes de validation par écho défini par l'objet cabhCtpPingNumPkts, ET mémoriser le résultat dans l'objet cabhCtpPingAvgRTT. Lorsqu'il exécute l'utilitaire de validation par écho, le portail CTP DOIT déterminer le nombre d'aller-retour minimum et maximum entre le service PS et le dispositif IP de réseau LAN, pour le nombre de requêtes de validation par écho défini par cabhCtpPingNumPkts, et mémoriser les résultats respectivement dans l'objet cabhCtpPingMinRTT et l'objet cabhCtpPingMaxRTT.

Si une erreur de protocole ICMP se produit au cours de l'exécution de l'utilitaire de validation par écho, le portail CTP DOIT incrémenter la valeur de l'objet cabhCtpPingNumIcmpError ET journaliser cette erreur dans l'objet cabhCtpPingIcmpError. La dernière erreur ICMP qui se produit remplace la précédente par surécriture.

La charge utile des paquets transmis pendant l'exécution de l'utilitaire de validation par écho NE DEVRAIT PAS être constituée uniquement de zéros ou de uns.

Le portail CTP DOIT réinitialiser à la valeur 0 chacun des objets cabhCtpPingNumSent, cabhCtpPingNumRecv, cabhCtpPingAvgRTT, cabhCtpPingMaxRTT, cabhCtpPingMinRTT, cabhCtpPingNumIcmpError et cabhCtpPingIcmpError lorsque l'utilitaire de validation par écho est lancé (c'est-à-dire lorsque la valeur de l'objet cabhCtpPingControl est mise à start(1)).

Le temps RTT de l'utilitaire de validation par écho est mesuré dans le service PS en tant que durée écoulée entre le moment où le dernier bit de chaque paquet est envoyé par l'utilitaire de validation par écho et le moment où le dernier bit de ce paquet est reçu.

Le portail CTP DOIT autoriser le réglage de l'adresse IP de destination de l'utilitaire de validation par écho (objet cabhCtpPingDestIp) à toute adresse IPv4 valide de tout dispositif IP de réseau LAN accessible au moyen de toute interface LAN du PS exécutant l'utilitaire de validation par écho du portail CTP.

L'utilitaire de validation par écho NE DOIT PAS générer de paquets à la sortie d'une quelconque interface avec un réseau WAN.

Le portail CTP NE DOIT PAS utiliser une quelconque adresse IP comme adresse IP de source de l'utilitaire de validation par écho (objet cabhCtpPingSrcIp) à l'exception d'une adresse IP actuelle et valide du réseau WAN-Data du PS (c'est-à-dire une valeur active de l'objet cabhCdpWanDataAddrIp) OU une adresse IP actuelle et valide de l'interface avec le réseau LAN du PS. Si une valeur non valide est configurée pour l'objet cabhCtpPingSrcIp, le portail CTP DOIT traiter l'exécution de l'essai comme un cas abandonné et régler à la valeur 'aborted' l'objet cabhCtpPingStatus indiquant le statut de l'utilitaire de validation par écho puis signaler l'événement approprié (voir le Tableau B.1).

6.5 Rapport d'événement

Le mécanisme de rapport et de commande d'événements utilisé est celui du document RFC 2669, qui définit un format normalisé pour les informations de rapport d'événement, sans considération du type de message, y compris un tableau d'enregistrement des événements locaux dans lequel certaines entrées vont persister d'un réamorçage à l'autre du service portail. Noter que des événements peuvent être produits par une partie quelconque d'un service portail, mais que le portail

CMP enregistre et/ou rapporte les événements soit localement ou dans un serveur de journalisation du système (Syslog) ou dans un serveur de transferts.

6.5.1 Notification d'événement

Le service portail DOIT produire des événements asynchrones qui indiquent les événements et situations importants comme spécifié à l'Annexe B (voir l'Annexe B). Les événements peuvent être mémorisés dans un enregistreur d'événements interne, mémorisés dans une mémoire non volatile, rapportés à d'autres entités du protocole SNMP (comme des messages TRAP ou INFORM du protocole SNMP), ou envoyés en tant que message d'événement SYSLOG à un serveur SYSLOG dont l'adresse IP est transmise dans l'option 7 du message OFFER en protocole DHCP reçu du serveur DHCP de tête de réseau par l'intermédiaire de l'interface PS/WAN-Man.

Le service portail DOIT accepter les mécanismes de notification d'événement suivants:

- enregistrement d'événements locaux lorsque certaines entrées contenues dans le journal local peuvent être identifiées comme persistant après un réamorçage du service portail;
- messages TRAP et INFORM du protocole SNMP;
- journal SYSLOG.

La notification d'événement par le service portail est entièrement configurable. Le service portail DOIT implémenter la table docsDevEvControlTable du document RFC 2669 afin de contrôler la signalisation des événements. Les valeurs activées par fanion (bits) suivantes pour l'objet docsDevEvReporting du document RFC 2669 DOIVENT être acceptées par le service portail:

- 1: local-nonvolatile(0)
- 2: traps(1)
- 3: syslog(2)
- 4: local-volatile(3)

Les messages de demande SET (*mise à jour*) du protocole SNMP envoyés à l'objet docsDevEvReporting du document RFC 2669 avec les valeurs suivantes DOIVENT résulter en une erreur "Valeur erronée" pour les unités PDU du protocole SNMP:

- 0x20 = syslog seulement
- 0x40 = transfert seulement
- 0x60 = (transfert + syslog) seulement

Un événement rapporté par message TRAP, SYSLOG ou INFORM DOIT générer aussi une entrée d'enregistrement local, volatile ou non volatile selon le Tableau 6-19 et comme décrit au § 6.5.1.1.

6.5.1.1 Enregistrement d'événement local

Le service portail DOIT maintenir un seul tableau d'événements d'enregistrement local qui contient les événements mémorisés à la fois locaux-volatiles et locaux-non volatiles. Les événements mémorisés comme événements locaux non volatiles DOIVENT persister au-delà des réamorçages du service portail. Le tableau d'événements d'enregistrement local DOIT être organisé comme une mémoire tampon cyclique avec un minimum de dix entrées. Le tableau unique d'événements d'enregistrement local DOIT être accessible par l'intermédiaire de la table docsDevEventTable comme défini dans RFC 2669.

Les descriptions d'événement DOIVENT apparaître en anglais. Les descriptions d'événement NE DOIVENT PAS dépasser 255 octets, ce qui est le maximum défini pour la chaîne SnmpAdminString.

L'identificateur d'événement (*EventId*) est un entier arithmétique de 32 bits. Les identificateurs EventId allant de 0 à ($2^{31} - 1$) sont réservés. L'identificateur EventId DOIT être converti à partir des codes d'erreur définis à l'Annexe B. Les identificateurs EventId allant de 2^{31} à ($2^{32} - 1$) DOIVENT être utilisés comme des identificateurs EventId spécifiques du vendeur au moyen du format suivant:

- le bit 31 est activé afin d'indiquer un événement propre au vendeur;
- les bits 30 à 16 contiennent les 15 bits inférieurs du numéro d'entreprise SNMP du vendeur;
- les bits 15 à 0 sont utilisés par le vendeur afin de numéroter ses événements.

L'objet docsDevEvIndex du document RFC 2669 sert à ordonner plus ou moins les événements dans le journal. Le marquage des événements d'enregistrement local comme étant de type local-volatile ou local-non volatile nécessite une méthode afin de synchroniser les valeurs de l'objet docsDevEvIndex entre ces deux types d'événements après un réamorçage du service portail. Après un réamorçage du service portail afin de synchroniser les valeurs de l'objet docsDevEvIndex pour les événements volatiles et non volatiles, on DOIT utiliser la procédure suivante:

- les valeurs de l'objet docsDevEvIndex pour les événements d'enregistrement local marqués comme étant de type local-non volatile DOIVENT être renumérotées en commençant par 1;
- l'enregistrement local DOIT être initialisé ensuite avec les événements marqués comme étant de type local-non volatile dans l'ordre qu'ils avaient immédiatement avant le réamorçage;
- les événements subséquemment mémorisés dans le journal local, qu'ils soient marqués comme étant de type local-volatile ou de type local-non volatile, DOIVENT utiliser des valeurs croissantes de l'objet docsDevEvIndex.

Une réinitialisation de l'enregistrement local lancée au moyen d'une demande SNMP de mise à jour (SET) de l'objet RFC 2669 docsDevEvControl DOIT supprimer tous les événements de l'enregistrement local, y compris les événements de journal marqués à la fois comme étant de type local-volatile et de type local-non volatile.

6.5.1.2 Messages TRAP et INFORM du protocole SNMP

Le service portail DOIT accepter l'unité PDU de transfert du protocole SNMP comme décrit dans RFC 2576. Le service portail DOIT accepter l'unité PDU INFORM du protocole SNMP comme décrit dans RFC 2576. Le message INFORM est une variante de transfert exigeant du serveur de réception qu'il accuse réception de l'arrivée d'une unité PDU de demande InformRequest avec une unité PDU de réponse InformResponse.

Lorsqu'un transfert normalisé en protocole SNMP est activé dans le service portail, celui-ci DOIT envoyer des notifications pour chaque événement de cette catégorie dont la priorité est soit "erreur" soit "notice".

Le service portail PEUT accepter des événements spécifiques du vendeur. S'ils sont acceptés, les événements de services portail spécifiques du vendeur communicables par message TRAP du protocole SNMP DOIVENT être décrits dans une base MIB privée qui est distribuée avec le service portail. Lors de la définition d'un transfert SNMP propre au vendeur, la déclaration OBJECTS de la définition du transfert privé DEVRAIT contenir au moins les objets décrits ci-dessous:

- EvLevel;
- EvIdText;
- seuil d'événement (s'il y en a un pour le transfert);
- IfPhysAddress (adresse physique associée à l'adresse IP du réseau WAN-Man du service portail).

D'autres objets peuvent être, au besoin, contenus dans la déclaration OBJECTS.

6.5.1.3 Messages SYSLOG

Les messages SYSLOG produits par le service portail DOIVENT être du format suivant:

<niveau>PortalServicesElement[vendeur]: <eventId> texte

où:

niveau – Présentation en caractères ASCII de la priorité de l'événement, incluse entre chevrons, qui est construite comme l'opérateur OU au niveau du bit de la fonction par défaut (128) et de la priorité d'événement (0 à 7). Le niveau résultant est compris entre 128 et 135.

vendeur – Nom du vendeur pour les messages SYSLOG spécifiques du vendeur ou "IPCABLE2HOME" pour les messages normalisés IPCable2Home.

EventId – Présentation en caractères ASCII du nombre entier INTEGER en format décimal, inclus entre chevrons, qui identifie de façon univoque le type d'événement. Cet identificateur EventID DOIT être le nombre qui a été mémorisé dans l'objet docsDevEvId de la table docsDevEventTable. Pour les événements normalisés IPCable2Home, ce nombre est converti à partir du code d'erreur selon les règles ci-après:

- c'est un nombre décimal à huit chiffres;
- les deux premiers chiffres (de gauche) constituent le code ASCII (décimal) de la lettre figurant dans le code d'erreur;
- les quatre chiffres suivants constituent les 2 ou 3 chiffres situés entre la lettre et le point du code d'erreur, l'espace vide à gauche étant rempli avec des zéros;
- les deux derniers chiffres constituent le nombre situé après le point dans le code d'erreur, l'espace vide à gauche étant rempli avec des zéros.

Par exemple, l'événement D04.2 est converti en 68000402, et l'événement I114.1 est converti en 73011401.

Noter que cette notion n'utilise qu'une petite partie d'espace numérique disponible qui est réservé pour IPCable2Home (0 à $2^{31} – 1$). La première lettre d'un code d'erreur est toujours en majuscule.

texte – Pour les messages IPCable2Home normalisés, cette chaîne DOIT avoir la description textuelle définie à l'Annexe B.

Exemple d'événement syslog pour l'événement D04.2: "Heure actuelle reçue en format non valide":

<132>Portal Services Element[IPCable2Home]: <68000402> Heure actuelle reçue en format non valide.

Dans l'exemple ci-dessus, le nombre 68000402 est celui qui a été attribué à cet événement particulier par le système IPCable2Home.

6.5.2 Format des événements

Les messages d'événement de gestion PEUVENT contenir l'une quelconque des informations suivantes:

- compteur d'événements – Indicateur de la séquence d'événements;
- heure d'événement – Heure d'apparition de l'événement;
- priorité d'événement – Sévérité de la condition. Le document RFC 2669 définit huit niveaux de sévérité. La sévérité d'événement par défaut peut être remplacée par une valeur différente pour chaque événement donné via l'interface de protocole SNMP;
- numéro d'entreprise de l'événement – Ce numéro identifie un événement soit comme étant normalisé soit comme étant défini par le vendeur;

- identificateur d'événement – Identifie l'événement exact lorsqu'il est combiné avec le numéro d'entreprise de l'événement. Les vendeurs définissent leurs propres identificateurs d'événement. Les événements de gestion normalisés selon IPCable2Home sont définis à l'Annexe B. Chaque événement de gestion décrit dans l'annexe reçoit un identificateur d'événement;
- texte de l'événement – Décrit l'événement sous une forme lisible par l'homme;
- adresse de commande MAC d'interface PS/WAN-Man – Décrit l'adresse de couche MAC de l'élément PS utilisé pour la gestion du bloc;
- adresse de commande MAC d'interface PS/WAN-Data – Décrit l'adresse de couche MAC de l'élément PS utilisé pour la gestion des données.

Le format exact de ces informations pour les messages TRAP et INFORM est défini à l'Annexe B. Le format des messages SYSLOG est défini dans la partie du présent paragraphe qui concerne les exigences.

6.5.2.1 Priorités d'événement

Le document RFC 2669 définit huit différents niveaux de priorité et les mécanismes de rapport correspondants pour chaque niveau. Les événements normalisés spécifiés dans la présente Recommandation utilisent ces niveaux de priorité.

Evénement d'urgence (priorité 1)

Réservé aux erreurs "fatales" de matériel ou de logiciel spécifiques du vendeur qui empêchent le fonctionnement normal du système et causent le réamorçage du système de rapport. Chaque vendeur peut définir son propre ensemble d'événements d'urgence. Des exemples de tels événements pourraient être "pas de mémoire tampon disponible", "échec des essais de mémoire", etc.

Evénement d'alerte (priorité 2)

Echec sérieux qui cause le réamorçage du système mais ce réamorçage n'est pas causé par un dysfonctionnement du matériel ou du logiciel. Après reprise sur l'événement, le système DOIT envoyer la notification de démarrage à froid/chaud.

Evénement critique (priorité 3)

Echec sérieux qui empêche le dispositif de transmettre des données mais dont il peut se remettre sans réamorçage du système. Après reprise sur événement critique, le service portail DOIT envoyer la notification de liaison activée. Des exemples de tels événements peuvent être des problèmes de fichier de configuration PS ou l'incapacité à obtenir une adresse IP par protocole DHCP.

Evénement d'erreur (priorité 4)

Echec qui pourrait interrompre le flux normal de données mais ne cause pas de réamorçage. Les événements d'erreur peuvent être rapportés en temps réel au moyen du mécanisme TRAP ou SYSLOG.

Evénement d'avertissement (priorité 5)

Echec qui pourrait interrompre le flux normal de données. Le rapport par messages SYSLOG et TRAP est activé par défaut pour ce niveau.

Evénement de notice (priorité 6)

Evénement d'importance qui n'est pas un échec et qui pourrait être rapporté en temps réel au moyen du mécanisme TRAP ou SYSLOG. Des exemples des événements NOTICE sont "Démarrage à froid", "Démarrage à chaud', "Liaison activée" et "Mise à jour logicielle réussie".

Evénement d'information (priorité 7)

Evénement d'importance qui n'est pas un échec mais qui pourrait être utile afin de garder la trace du fonctionnement normal du dispositif.

Evénement de débogage (priorité 8)

Priorité réservée à des événements non critiques, propres au vendeur.

La priorité associée aux événements normalisés NE DOIT PAS être changée.

Le Tableau 6-19 indique les types de notification par défaut pour les diverses priorités d'événement. Le service portail DOIT implémenter les types de notification par défaut pour les huit priorités d'événement. Par exemple, le type de notification par défaut pour les événements Urgence et Alerte consiste à les placer dans le journal local comme entrées non volatiles.

Tableau 6-19/J.191 – Types de notification par défaut pour les priorités d'événements du service PS

Priorité d'événement	Local-non volatile (bit-0)	Message TRAP du SNMP (bit-1)	Message SYSLOG (bit-2)	Local-volatile (bit-3)	Note
1) Urgence	Oui	Non	Non	Non	Propre au vendeur
2) Alerte	Oui	Non	Non	Non	Normalisé
3) Critique	Oui	Non	Non	Non	Normalisé
4) Erreur	Oui	Oui	Oui	Non	Normalisé
5) Avertissement	Oui	Oui	Oui	Non	Normalisé
6) Notice	Non	Oui	Oui	Oui	Normalisé
7) Information	Non	Non	Non	Non	Normalisé et propre au vendeur
8) Débogage	Non	Non	Non	Non	Propre au vendeur

Le service PS DOIT prendre en charge la capacité d'être configuré de façon à générer tous les types de notification pour chacun des niveaux de priorité d'événement énumérés dans le Tableau 6-19.

Tableau 6-20/J.191 – Niveau minimal d'acceptation de type de notification par priorité d'événement dans le service PS

Priorité d'événement	Local-non volatile (bit-0)	Message TRAP du SNMP (bit-1)	SYSLOG (bit-2)	Local-volatile (bit-3)	Note
1) Urgence	Oui	Oui	Oui	Oui	Propre au vendeur
2) Alerte	Oui	Oui	Oui	Oui	Normalisé
3) Critique	Oui	Oui	Oui	Oui	Normalisé
4) Erreur		Oui	Oui	Oui	Normalisé
5) Avertissement		Oui	Oui	Oui	Normalisé
6) Notice		Oui	Oui	Oui	Normalisé
7) Information		Oui	Oui	Oui	Normalisé et propre au vendeur
8) Débogage		Oui	Oui	Oui	Propre au vendeur

6.5.2.2 Evénements normalisés

Le service portail DOIT envoyer les transferts génériques suivants en protocole SNMP, comme défini dans les documents RFC 3418 et RFC 2863:

- coldStart [RFC 3418] (*démarrage à froid*);
- linkUp [RFC 2863] (*liaison activée*);
- linkDown [RFC 2863] (*liaison désactivée*);
- SNMP authentication-Failure [RFC 3418] (*échec d'authentification SNMP*).

Le service portail DOIT être capable de produire des notifications d'événement fondées sur la liste d'événements normalisés de l'Annexe B.

6.5.3 Ralentissement et limitation d'événements

Le service portail DOIT accepter le ralentissement et la limitation des événements TRAP/INFORM et SYSLOG du protocole SNMP comme décrit dans RFC 2669.

Le service portail DOIT considérer que les événements sont identiques si leurs identificateurs EventId sont identiques.

Le document RFC 2669 spécifie quatre états de ralentissement:

- unconstrained(1) (sans contraintes) provoque la transmission des transferts TRAP et des messages SYSLOG sans considération du réglage des seuils;
- maintainBelowThreshold(2) (maintien au-dessous du seuil) provoque la suppression de la transmission des transferts TRAP et des messages SYSLOG de façon que le nombre de transferts ne dépasse pas le seuil;
- stopAtThreshold(3) (maintien au niveau du seuil) provoque la cessation de la transmission de transfert au niveau du seuil et sa non-reprise jusqu'à ordre contraire;
- inhibited(4) (inhibition) provoque la suppression de toute transmission de transferts TRAP et de messages SYSLOG.

Un événement isolé DOIT être traité comme un événement unique en termes de comptage d'événements de seuil, c'est-à-dire qu'un événement causant à la fois un transfert TRAP et un message SYSLOG est toujours traité comme un événement unique.

6.5.4 Rapport d'événement de téléchargement sécurisé de logiciel

Le Tableau B.1, Format et contenu des événements, de l'enregistrement SYSLOG et des transferts TRAP du protocole SNMP, décrit les événements associés aux mises à jour logicielles des services PS selon trois catégories: initialisation de mise à jour logicielle (SW UPGRADE INIT), échec général de mise à jour logicielle, et succès de mise à jour logicielle. Ces événements ne s'appliquent qu'au service PS autonome car la mise à jour logicielle (également appelée *téléchargement sécurisé de logiciel*) d'un service PS imbriqué est régie et gérée par le câblo-modem. Le § 11.3.7.1 définit des exigences de téléchargement sécurisé de logiciel pour les deux classes d'éléments de services PS. Le service PS imbriqué, tel que défini dans le § 5.1.3.1 NE DOIT PAS générer d'événements de la catégorie "Initialisation de mise à jour logicielle" (SW UPGRADE INIT), de la catégorie "Echec général de mise à jour logicielle" (SW UPGRADE GENERAL FAILURE) ou "Succès de mise à jour logicielle" (SW UPGRADE SUCCESS) selon le Tableau B.1.

7 Utilitaires d'approvisionnement

7.1 Introduction/aperçu général

L'élément de services PS et les dispositifs IP de réseau LAN DOIVENT être correctement initialisés et configurés afin d'échanger des informations significatives l'un avec l'autre et avec les éléments

connectés au réseau câblé et l'Internet. Les utilitaires d'approvisionnement IPCable2Home permettent à cette initialisation et à cette configuration de se produire de façon transparente et avec une intervention minimale de l'utilisateur. Ils permettent aussi aux câblo-opérateurs d'apporter de la valeur ajoutée aux abonnés aux services de données à haut débit en définissant les processus par lesquels le câblo-opérateur peut faciliter et personnaliser l'initialisation et la configuration du service portail et du dispositif IP de réseau LAN. Les trois utilitaires d'approvisionnement définis pour accomplir cette tâche sont énumérés ci-dessous:

- fonction de portail DHCP de câble (CDP, *cable DHCP portal*) dans l'élément de services PS;
- utilitaire de configuration globale des services PS (BPSC, *bulk PS configuration*);
- client d'heure actuelle dans l'élément de services PS.

7.1.1 Modes d'approvisionnement

Deux modes d'approvisionnement sont acceptés: le mode d'approvisionnement DHCP (mode DHCP) et le mode d'approvisionnement SNMP (mode SNMP). Ces deux modes d'approvisionnement sont comparés dans le Tableau 7-1.

Tableau 7-1/J.191 – Modes d'approvisionnement

	Mode DHCP	**Mode SNMP**
Déclenchement du fichier de configuration PS	Déclenché par la présence d'informations de serveur TFTP dans le message DHCP	Déclenché par le système NMS via un message SNMP
Exigences du fichier de configuration PS	Le téléchargement du fichier de configuration PS est exigé	Le téléchargement du fichier de configuration PS n'est pas exigé

Le comportement spécifié des utilitaires d'approvisionnement dépend du mode d'approvisionnement dans lequel fonctionne le service portail.

Le § 13 décrit la séquence des événements pour chacun des deux modes d'approvisionnement.

7.1.2 Architecture d'approvisionnement

La Figure 7-1 illustre l'architecture d'approvisionnement. Les éléments de services portail vont interagir avec les fonctions de serveur dans le réseau câblé à l'interface avec l'hybride HFC, ou avec les dispositifs IP de réseau LAN afin de répondre aux directives de conception du système énumérées au § 7.2.1.

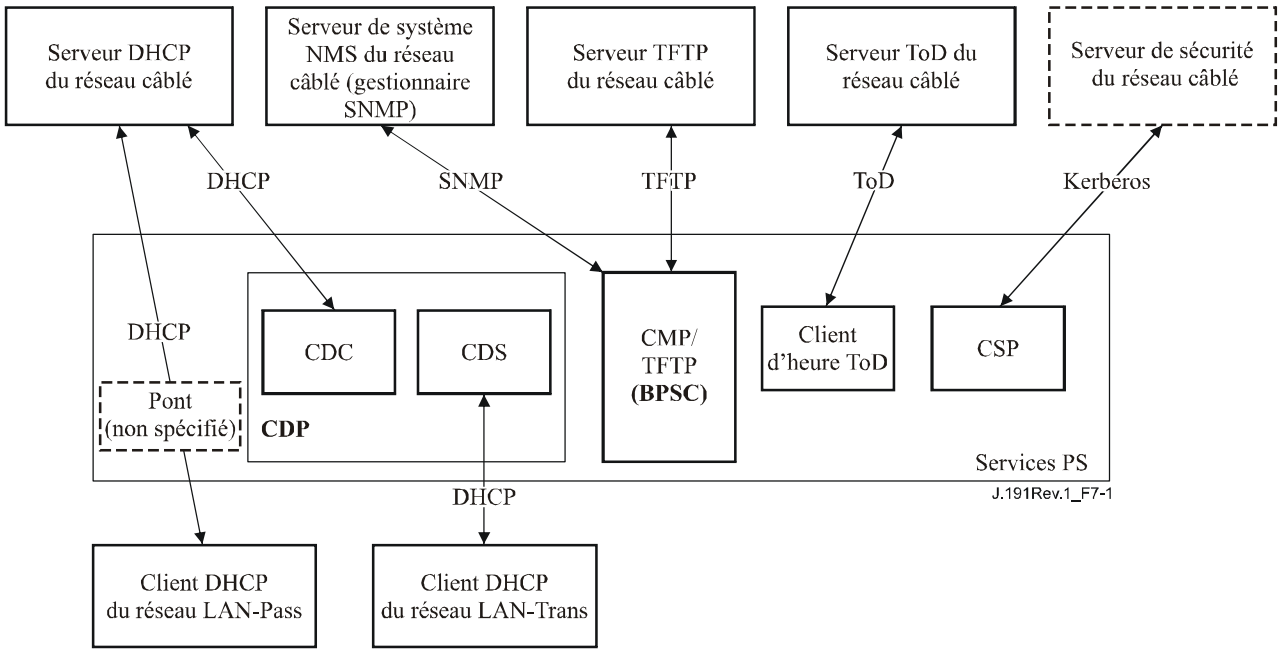


Figure 7-1/J.191 – Architecture d'approvisionnement

7.1.3 Objectifs

Les objectifs du portail DHCP par câble sont les suivants:

- attribuer, par protocole DHCP, des adresses IP aux dispositifs IP de réseau LAN conformément aux règles spécifiées dans le présent paragraphe;
- acquérir, par protocole DHCP, des adresses IP pour les interfaces WAN des éléments de services portail conformément aux règles spécifiées dans le présent paragraphe.

Les objectifs de l'utilitaire de configuration globale des services PS sont les suivants:

- télécharger et traiter les fichiers de configuration.

Les objectifs du client d'heure actuelle sont les suivants:

- synchroniser l'horloge dans l'élément de services PS avec celle de la tête de réseau.

7.1.4 Hypothèses

Les hypothèses de fonctionnement du portail DHCP par câble sont les suivantes:

1) les dispositifs IP de réseau LAN implémentent un client DHCP comme défini par RFC 2131;
2) le système d'approvisionnement du réseau câblé implémente un serveur DHCP comme défini par RFC 2131;
3) si le serveur DHCP du système d'approvisionnement du réseau câblé accepte l'option 61 (option d'identificateur de client) du protocole DHCP, les interfaces IP de réseau WAN-Man et toutes les interfaces IP de réseau WAN-Data peuvent partager une adresse de commande MAC commune;
4) les dispositifs IP de réseau LAN peuvent accepter diverses options DHCP et diverses extensions BOOTP de vendeur, permises par RFC 2132.

Les hypothèses de fonctionnement de l'utilitaire de configuration globale des services PS sont les suivantes:

– la configuration globale des services PS sera réalisée par téléchargement d'un fichier de configuration PS contenant un ou plusieurs paramètres.

Les hypothèses de fonctionnement du client d'heure actuelle sont les suivantes:

– le serveur DHCP de tête de réseau fournira une option DHCP à l'interface WAN-Man afin de désigner un serveur temporel fonctionnant au sein du réseau de tête de réseau.

7.2 Architecture de portail DHCP du câble

Le portail DHCP du câble (CDP) est un des trois utilitaires d'approvisionnement présentés au § 7.1. Le présent paragraphe décrit les directives de conception du système, la description du système et les exigences relatives au portail CDP.

7.2.1 Directives de conception du système de portail DHCP du câble

Les directives de conception suivantes (Tableau 7-2) régissent les fonctionnalités définies pour le portail CDP:

Tableau 7-2/J.191 – Directives de conception du système de portail CDP

Numéro	Directives de conception du système de portail CDP
CDP 1	Les mécanismes d'adressage seront sous le contrôle de l'opérateur, et fourniront au câblo-opérateur la connaissance des éléments de réseau IPCable2Home et des dispositifs IP de réseau LAN, ainsi que l'accessibilité à ces éléments et dispositifs.
CDP 2	Les processus d'acquisition et de gestion d'adresse n'exigeront pas d'intervention humaine (en supposant qu'un compte d'utilisateur/de foyer a déjà été établi).
CDP 3	L'acquisition et la gestion d'adresse seront échelonnables afin de prendre en charge l'augmentation attendue du nombre de dispositifs IP de réseau LAN.
CDP 4	Il est préférable que les adresses IP de réseau LAN restent les mêmes après des événements tels qu'un cycle d'alimentation ou un changement de fournisseur de services Internet.
CDP 5	On fournira un mécanisme permettant de surveiller et de contrôler le nombre de dispositifs IP de réseau LAN situés dans le secteur LAN-Trans.
CDP 6	Au domicile, les communications continueront de fonctionner comme prévu pendant les périodes de panne du serveur d'adresses de la tête de réseau. La prise en charge de l'adressage sera assurée pour les dispositifs IP de réseau LAN nouvellement ajoutés et pour les expirations d'adresses pendant les pannes de serveur d'adresses distant.
CDP 7	Les adresses IP seront conservées si possible (aussi bien les adresses acheminables mondialement que les adresses privées de gestion de réseau câblé).

7.2.2 Description du système de portail DHCP du câble

Le portail DHCP du câble (CDP) est l'entité logique responsable des activités d'adressage IPCable2Home. Les responsabilités du portail CDP pour la demande d'adresse et l'attribution d'adresse sont les suivantes dans l'environnement IPCable2Home:

- l'attribution d'adresse IP, la maintenance d'adresse IP et la remise des paramètres de configuration (par protocole DHCP) aux dispositifs IP de réseau LAN situés dans le secteur d'adresses LAN-Trans;
- l'acquisition d'une adresse IP de réseau WAN-Man et de zéro, une ou plusieurs adresses IP de réseau WAN-Data et des paramètres associés de configuration DHCP pour l'élément de services PS;
- fournir des informations au portail de nommage du câble (CNP) afin de prendre en charge des services de nom de serveur de dispositif IP de réseau LAN.

Le service PS conserve deux adresses de matériel, dont l'une doit servir à acquérir une adresse IP aux fins de gestion et dont l'autre peut servir à acquérir une ou plusieurs adresse(s) IP pour des

données. Afin d'empêcher la simulation d'une adresse de matériel, le service PS ne permet pas la modification de l'une quelconque des deux adresses de matériel.

L'élément de services PS exige une adresse IP dans le réseau LAN résidentiel pour son rôle de routeur de trafic résidentiel (voir § 8), de serveur DHCP (CDS), et de serveur DNS (voir § 9). Pour chacune de ces trois fonctions (double serveur d'élément de services PS et routeur), une adresse IP de réseau LAN est sauvegardée dans la base de données du service portail. Chaque adresse peut être atteinte au moyen d'un objet de base MIB différent, dont la liste figure ci-dessous et dans le Tableau 7-2.

Adresse de routeur (passerelle par défaut)	cabhCdpServerRouter
Adresse de service de nom de domaine (DNS)	cabhCdpServerDnsAddress
Adresse de serveur de configuration dynamique d'hôte (DHCP) (serveur CDS)	cabhCdpServerDhcpAddress

La valeur par défaut de l'objet cabhCdpServerRouter est 192.168.0.1. Les valeurs par défaut de l'objet cabhCdpServerDnsAddress et de l'objet cabhCdpServerDhcpAddress sont égales à la valeur de l'objet cabhCdpServerRouter.

Comme indiqué à la Figure 7-2, les fonctionnalités du portail CDP sont imbriquées dans deux éléments fonctionnels résidant au sein du portail CDP: le serveur DHCP du câble (CDS) et le client DHCP du câble (client CDC).

La Figure 7-2 illustre aussi l'interaction entre les composants du portail CDP et les secteurs d'adresses présentés au § 5. Le client CDC échange des messages DHCP avec le serveur DHCP dans le réseau câblé (secteur d'adresses de gestion de réseau WAN) afin d'acquérir une adresse IP et des options DHCP pour le service portail, aux fins de la gestion. Le client CDC peut aussi échanger des messages DHCP avec le serveur DHCP dans le réseau câblé (secteur d'adresses de réseau WAN-Data) afin d'acquérir zéro, une ou plusieurs adresses IP au compte des dispositifs IP de réseau LAN situés dans le secteur LAN-Trans. Le serveur CDS échange des messages DHCP avec les dispositifs IP de réseau LAN situés dans le secteur LAN-Trans afin d'attribuer des adresses IP privées aux clients DHCP implantés dans ces dispositifs IP de réseau LAN, de leur accorder des connexions louées et de leur fournir, le cas échéant, des options DHCP. Les dispositifs IP de réseau LAN situés dans le secteur LAN-Pass reçoivent leurs adresses IP, leurs connexions louées, et leurs options DHCP directement du serveur DHCP implanté dans le réseau câblé. Le portail CDP dérive simplement les messages DHCP entre le serveur DHCP implanté dans le réseau câblé et les dispositifs IP de réseau LAN implantés dans le secteur LAN-Pass.

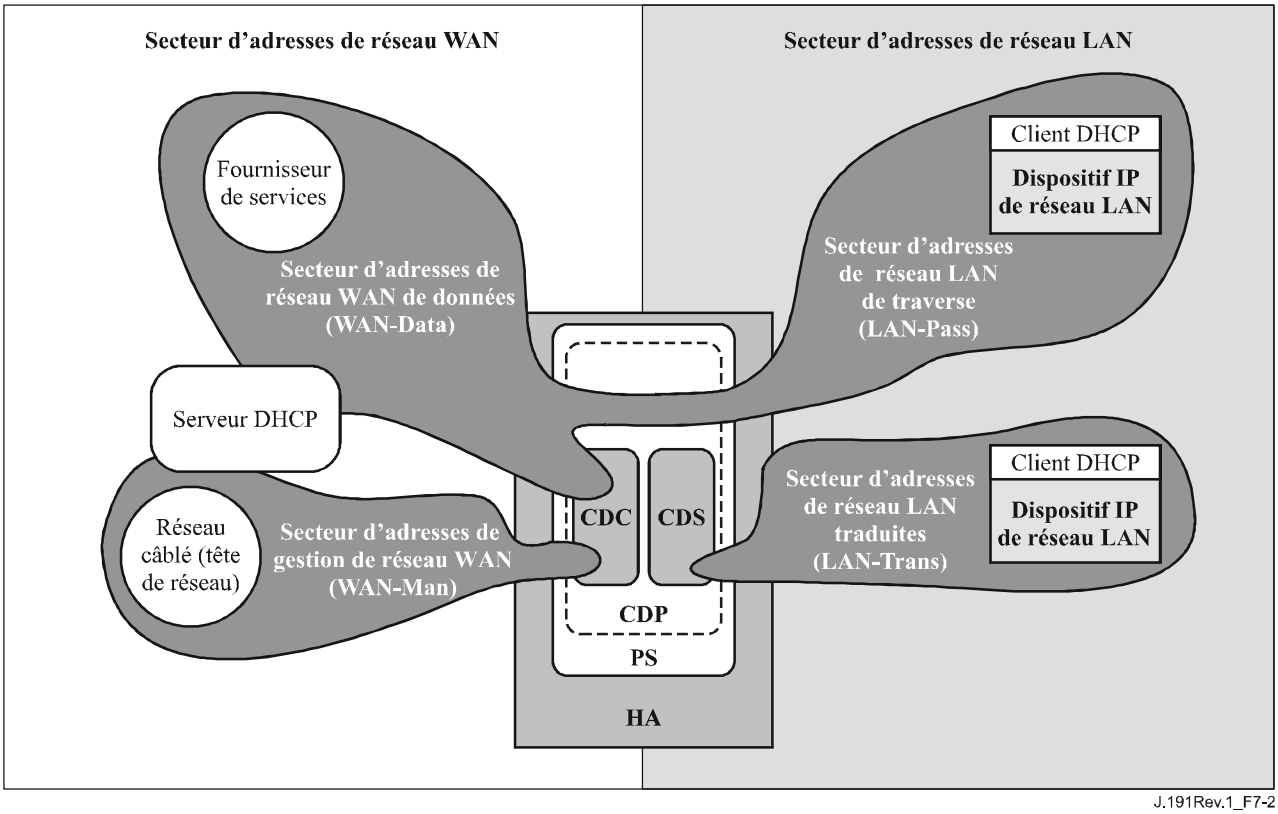


Figure 7-2/J.191 – Fonctions du portail CDP

7.2.2.1 Description du système de serveur CDS

Le serveur CDS est un serveur DHCP normalisé comme défini dans RFC 2131. Ses responsabilités sont les suivantes:

- le serveur CDS attribue les adresses et délivre les paramètres de configuration DHCP aux dispositifs IP de réseau LAN recevant une adresse dans le secteur d'adresses LAN-Trans. Le serveur CDS apprend les options DHCP du système NMS et fournit ces options DHCP aux dispositifs IP de réseau LAN. Si les options DHCP n'ont pas été fournies par le système NMS (par exemple lorsque le service portail s'amorce lors d'une panne du câble), le serveur CDS se fonde sur les valeurs par défaut intégrées (DefVals) pour les options nécessaires;
- le serveur CDS est capable de fournir des services d'adressage aux dispositifs IP de réseau LAN, indépendamment de l'état de connexité du réseau WAN;
- le nombre d'adresses fournies par le serveur CDS aux dispositifs IP de réseau LAN est contrôlable par le système NMS. Le comportement du serveur CDS lorsque la limite de réglage par câblo-opérateur est dépassée est aussi configurable via le système NMS. Les actions de serveur CDS possibles lorsque la limite est dépassée sont les suivantes:

  1) attribuer une adresse IP de réseau LAN-Trans et traiter l'interconnexion WAN-LAN par conversion CAT comme cela se serait produit normalement si la limite n'avait pas été dépassée;

  2) ne pas attribuer d'adresse aux dispositifs IP de réseau LAN demandeurs.

     Un réglage à 0 du seuil d'adresses indique le seuil maximal possible pour la réserve d'adresses IP de réseau LAN-Trans définie par les valeurs "start" (début) (objet cabhCdpLanPoolStart) et "end" (fin) (objet cabhCdpLanPoolEnd) de réserve;

- en l'absence d'informations sur l'heure de la part du serveur temporel (ToD, *time of day*), le serveur CDS utilise la date de début par défaut du service portail 00:00:00 (minuit) GMT le 1er janvier 1970, met à jour l'heure d'expiration pour toutes connexions louées actives dans le secteur LAN-Trans afin de se resynchroniser avec les clients DHCP dans les dispositifs IP de réseau LAN, et assure la maintenance des connexions louées sur la base de ce point de départ jusqu'à ce que le service portail se synchronise avec le serveur temporel dans le réseau câblé;
- lors d'un amorçage du service PS, le serveur CDS reste inactif jusqu'à son activation par le service PS;
- si le mode primaire de traitement de paquet du service portail (objet cabhCapPrimaryMode) a été réglé à la traversée ET si le processus d'approvisionnement du service PS s'est achevé (ce qui est indiqué par l'objet cabhPsDevProvState = pass(1)), le serveur CDS est désactivé.

Les dispositifs IP de réseau LAN peuvent recevoir des adresses qui résident dans le secteur LAN-Pass. Comme indiqué à la Figure 7-2, les demandes d'adresse LAN-Pass sont servies par l'infrastructure d'adressage du réseau WAN, et non par le service portail. Les processus d'adressage LAN-Pass interviendront lorsque le service portail sera configuré pour fonctionner en mode de traversée ou en mode mixte de dérivation/acheminement (voir le § 8.2.2.2 pour plus de détails). Dans ces cas, les interactions DHCP surviendront directement entre les dispositifs IP de réseau LAN et les serveurs de tête de réseau. La présente Recommandation ne spécifie pas ce processus.

Tout au long de la présente Recommandation, les termes *attribution dynamique* et *attribution manuelle* sont utilisés comme défini dans RFC 2131. Les options DHCP fournies par le serveur CDS représenté par les objets cabhCdpServer contenus dans la base MIB du portail CDP sont des options DHCP qui peuvent être fournies par le système NMS et qui sont offertes par le serveur CDS aux dispositifs IP de réseau LAN munis d'une adresse LAN-Trans. Les options DHCP fournies par le serveur CDS représenté par les objets cabhCdpServer persistent après un cycle d'alimentation électrique du service portail et le système NMS peut établir, lire, écrire et supprimer ces objets. Les options DHCP fournies par le serveur CDS représenté par les objets cabhCdpServer sont conservées pendant les périodes de panne du câble et ces objets sont offerts aux dispositifs IP de réseau LAN munis d'une adresse LAN-Trans pendant les périodes de panne du câble. Le stockage persistant des options DHCP est cohérent avec la section 2.1 du document RFC 2131. Les valeurs par défaut des options DHCP fournies par le serveur CDS représenté par les objets cabhCdpServer sont définies au Tableau 7-2 et le système NMS peut réinitialiser à leurs valeurs par défaut les options DHCP fournies par le serveur CDS représenté par les objets cabhCdpServer, en récrivant l'objet cabhCdpSetToFactory de la base MIB.

Les objets de seuil d'adresses de serveur CDS (objets cabhCdpLanTrans) contiennent les paramètres de commande d'événement utilisés par le serveur CDS pour signaler au portail CMP l'ordre de générer une notification à destination du système de gestion de tête de réseau lorsque le nombre d'adresses LAN-Trans attribuées par le serveur CDS dépasse le seuil préétabli.

L'objet de compte d'adresses (objet cabhCdpLanTransCurCount) est une valeur indiquant le nombre d'adresses LAN-Trans attribuées par le serveur CDS qui ont des connexions louées DHCP actives.

L'objet de seuil d'adresses (objet cabhCdpLanTransThreshold) est une valeur qui indique le moment où une notification est générée à destination du système de gestion de tête du réseau. La notification est générée lorsque le serveur CDS attribue une adresse au dispositif IP de réseau LAN qui provoque un dépassement du seuil (objet cabhCdpLanTransThreshold) de compte d'adresses (objet cabhCdpLanTransCurCount).

L'action sur dépassement de seuil (objet cabhCdpLanTransAction) est l'action prise par le serveur CDS lorsque le compte d'adresses (objet cabhCdpLanTransCurCount) dépasse le seuil d'adresses (objet cabhCdpLanTransThreshold). Si l'action sur dépassement de seuil (objet

cabhCdpLanTransAction) permet des attributions d'adresses après que le compte a été dépassé, la notification est générée chaque fois qu'une adresse est attribuée. Les actions définies sont:

a) attribuer une adresse LAN-Trans comme en cas normal;

b) ne pas attribuer d'adresse au prochain dispositif IP de réseau LAN demandeur.

Le compte d'adresses (objet cabhCdpLanTransCurCount) continue d'être mis à jour pendant les périodes de panne du câble.

La base MIB du serveur CDS contient aussi les paramètres de début de groupe d'adresses (objet cabhCdpLanPoolStart) et de fin de groupe d'adresses (objet cabhCdpLanPoolEnd). Ces paramètres indiquent la gamme d'adresses qui, dans le secteur LAN-Trans, peuvent être attribuées par le serveur CDS aux dispositifs IP de réseau LAN.

Le tableau d'adresse LAN du portail CDP (objet cabhCdpLanAddrTable) contient la liste des paramètres associés aux adresses attribuées aux dispositifs IP de réseau LAN avec des adresses LAN-Trans. Ces paramètres sont les suivants:

1) les identificateurs du client selon la section 9.14 du document RFC 2132 (objet cabhCdpLanAddrClientID);

2) l'adresse IP de réseau LAN attribuée au client (objet cabhCdpLanAddrIp);

3) une indication précisant si l'adresse a été attribuée manuellement (via le portail CMP) ou automatiquement (via le portail CDP) (objet cabhCdpLanAddrConfig).

Le serveur CDS mémorise les informations d'identification du dispositif IP de réseau LAN situé dans l'objet cabhCdpLanAddrClientID de base MIB. Le serveur CDS utilise la valeur introduite dans le champ *chaddr* du message de demande DHCP envoyé par le dispositif IP de réseau LAN à cette fin.

Le serveur CDS crée une entrée de table de portail CDP (objet cabhCdpLanAddrTable) lorsqu'il attribue une adresse IP à un dispositif IP de réseau LAN. Le serveur CDS peut créer des entrées de table de portail CDP (objet cabhCdpLanAddrTable) pendant les périodes de panne du câble.

La table de portail CDP (objet cabhCdpLanAddrTable) entretient un temps de location DHCP pour chaque dispositif IP de réseau LAN.

Les entrées de table de portail CDP approvisionnées par le système NMS (objet cabhCdpLanAddrTable) sont conservées pendant les périodes de panne du câble et survivent aux cycles d'alimentation.

7.2.2.2 Description du système de client CDC

Le client CDC est un client DHCP normalisé comme défini dans RFC 2131. Ses responsabilités sont les suivantes:

- faire des demandes aux serveurs DHCP de tête du réseau pour l'acquisition des adresses dans le réseau WAN-Man et faire des demandes aux serveurs DHCP de tête de réseau pour l'acquisition d'adresses dans les secteurs d'adresses WAN-Data. Le client CDC lit de nombreux paramètres de configuration DHCP par câble et agit sur eux;
- le client CDC accepte l'acquisition d'une seule adresse IP de réseau WAN-Man et de zéro, une ou plusieurs d'adresses IP de réseau WAN-Data;
- le client CDC accepte l'option d'identificateur de classe du vendeur (option DHCP 60), l'option d'informations spécifiques du vendeur (option DHCP 43), et l'option d'identificateur de client (option DHCP 61);
- dans le cas par défaut, le client CDC acquerra une seule adresse IP pour un usage simultané par les interfaces IP de réseau WAN-Man et de réseau WAN-Data. Afin de minimiser les changements à apporter aux serveurs DHCP de tête de réseau existants, l'utilisation d'un

identificateur de client (option DHCP 61) par le client CDC n'est pas exigée dans ce cas par défaut.

Le portail CDP accepte diverses options DHCP et extensions BOOTP de vendeur, permises par RFC 2132.

L'option d'identificateur de classe du vendeur (option DHCP 60) définit une classe de dispositif spécifique. Dans l'environnement IPCable2Home, l'option d'identificateur de classe du vendeur contiendra la chaîne "IPCable2Home" afin d'identifier un élément logique de services portail dans l'environnement IPCable2Home chaque fois que le client CDC demande une adresse WAN-Man ou WAN-Data.

L'option d'informations spécifiques du vendeur (option DHCP 43) identifie plus précisément le type de dispositif et ses capacités. Elle décrit le type de composant qui fait la demande (imbriqué ou autonome, CM ou PS), les composants qui sont contenus dans le dispositif (CM, MTA, PS, etc.), et le numéro de série du dispositif. Elle permet aussi d'indiquer des paramètres spécifiques du dispositif. L'option DHCP 43 est décrite au § 7.2.3.3 avec ses sous-options.

Les Tableaux 7-4 et 7-5 contiennent des précisions sur les exigences de la prise en charge des options DHCP 60 et 43. Le Tableau 7-6 contient des détails sur d'autres options DHCP, facultatives et obligatoires.

Le paramètre de décompte d'adresses IP de réseau WAN-Data de la base MIB du portail CDP (objet cabhCdpWanDataIpAddrCount) est le nombre de locations d'adresse IP que le client CDC est tenu d'essayer d'acquérir pour le côté WAN des mappages de conversion NAT et NAPT. La valeur par défaut de l'objet cabhCdpWanDataIpAddrCount est zéro, ce qui signifie que, par défaut, le client CDC n'obtiendra qu'une seule adresse IP de réseau WAN-Man.

7.2.2.2.1 Option 61 du client DHCP par câble

L'élément de services PS peut avoir une ou plusieurs adresses IP de réseau WAN associées à une ou plusieurs interfaces de couche de liaison (par exemple, MAC). Le client CDC ne peut donc pas se reposer seulement sur une adresse de commande MAC comme unique valeur d'identificateur de client.

La présente Recommandation permet l'utilisation de l'option d'identificateur de client (option DHCP 61), section 9.14 du document RFC 2132, pour identifier de façon univoque l'interface WAN logique associée à une adresse IP particulière.

Le service PS est tenu d'avoir deux adresses de matériel: l'une servant à identifier de façon univoque l'interface logique WAN associée à l'adresse IP de réseau WAN-Man (adresse matérielle WAN-Man) et l'autre servant à identifier de façon univoque l'interface logique WAN associée à des adresses IP de réseau WAN-Data (adresse matérielle WAN-Data).

7.2.2.2.2 Modes des adresses de réseau WAN

Afin de permettre la compatibilité avec autant de systèmes d'approvisionnement de câblo-opérateur que possible, le client CDC prendra en charge les modes configurables suivants des adresses de réseau WAN:

mode 0 d'adresse WAN: l'élément de services PS utilise une seule adresse IP de réseau WAN, acquise par protocole DHCP au moyen de l'adresse matérielle du réseau WAN-Man. L'élément de services PS a une seule interface IP/WAN-Man et zéro interface IP/WAN-Data. Ce mode d'adresse n'est applicable que lorsque le mode de traitement primaire de paquet PS (objet cabhCapPrimaryMode) est mis à la valeur "traversée" (voir § 8.3.2). Le serveur DHCP de tête de réseau du câblo-opérateur n'a normalement pas besoin de modifications logicielles afin de prendre en charge ce mode d'adresse. En mode 0 d'adresse de réseau WAN, la valeur de l'objet cabhCdpWanDataIpAddrCount est zéro.

mode 1 d'adresse WAN: l'élément de services PS utilise une seule adresse IP de réseau WAN, acquise par protocole DHCP au moyen de l'adresse matérielle du réseau WAN-Man. L'élément de services PS a une seule interface IP/WAN-Man et une seule interface IP/WAN-Data. Ces deux interfaces se partagent une même adresse IP commune. Ce mode d'adresse n'est applicable que lorsque le mode de traitement primaire de paquet PS (objet cabhCapPrimaryMode) est mis à la valeur de traduction NAPT. Le serveur DHCP de tête de réseau du câblo-opérateur n'a normalement pas besoin de modifications logicielles afin de prendre en charge ce mode d'adresse. En mode 1 d'adresse de réseau WAN, la valeur de l'objet cabhCdpWanDataIpAddrCount est zéro.

mode 2 d'adresse de réseau WAN: l'élément de services PS acquiert une adresse IP de réseau WAN-Man au moyen de l'adresse matérielle unique de réseau WAN-Man. Il est ensuite configuré par le système NMS afin de demander une ou plusieurs adresse(s) IP unique(s) de réseau WAN-Data. L'élément de services PS possédera une seule interface avec le réseau WAN-Man et une ou plusieurs interface(s) IP avec le réseau WAN-Data. Toutes les adresses IP de réseau WAN-Data se partageront une même adresse matérielle qui sera unique par rapport à l'adresse matérielle du réseau WAN-Man. Les deux ou plus interfaces (une interface WAN-Man et une ou plusieurs interface(s) WAN-Data) possèdent chacune leur propre adresse IP non partagée. Le portail CDP est configuré par le câblo-opérateur de façon à fonctionner dans le mode 2 d'adresse de réseau WAN en écrivant une valeur différente de zéro dans l'objet cabhCdpWanDataIpAddrCount, au moyen du fichier de configuration PS ou d'une demande de mise à jour SNMP. Ce mode d'adresse est applicable lorsque le mode de traitement primaire de paquets PS (objet cabhCapPrimaryMode) est mis à la valeur de traduction NAPT ou NAT. Le serveur DHCP de tête de réseau du câblo-opérateur peut avoir besoin d'une modification logicielle afin de prendre également en charge les identificateurs de client (Option DHCP 61) de façon qu'il puisse attribuer de multiples adresses IP à l'adresse matérielle unique du réseau WAN-Data.

Il existe quatre scénarios possibles pour les adresses IP de réseau WAN-Data:

1) le service PS est configuré de façon à ne demander aucune nouvelle adresse IP de réseau WAN-Data. Aucun identificateur de client de réseau WAN-Data n'est nécessaire;

2) le service PS est configuré de façon à demander une ou plusieurs adresse(s) IP de réseau WAN-Data et il n'y a aucune entrée d'objet cabhCdpWanDataAddrClientId dans la base MIB du portail CDP. Le service PS est tenu de générer automatiquement autant d'identificateurs uniques de client du service WAN-Data qu'indiqué par la valeur de l'objet cabhCdpWanDataIpAddrCount;

3) le service PS est configuré de façon à demander une ou plusieurs adresse(s) IP de réseau et il y a au moins autant d'entrées d'objet cabhCdpWanDataAddrClientId configurées par l'opérateur qu'indiqué par la valeur de l'objet cabhCdpWanDataIpAddrCount, c'est-à-dire que l'opérateur a approvisionné un nombre suffisant de valeurs d'identificateur de client de réseau WAN-Data. Le service PS ne génère automatiquement aucun identificateur de client;

4) le service PS est configuré de façon à demander une ou plusieurs adresse(s) IP de réseau WAN-Data et il y a moins d'entrées d'objet cabhCdpWanDataAddrClientId configurées par l'opérateur qu'indiqué par la valeur de l'objet cabhCdpWanDataIpAddrCount, c'est-à-dire que l'opérateur a approvisionné quelques valeurs d'identification de client de réseau WAN-Data mais en nombre insuffisant. Le service PS est tenu de générer automatiquement un nombre suffisant d'identificateurs de client de réseau WAN-Data pour rendre le nombre total d'identificateurs uniques de client de réseau WAN-Data égal à la valeur de l'objet cabhCdpWanDataIpAddrCount.

Si le câblo-opérateur souhaite que le service PS obtienne une ou plusieurs adresse(s) IP de réseau WAN-Data distinctes de l'adresse IP du réseau WAN-Man, la procédure est la suivante. Dans tous les modes d'adresse de réseau WAN, le service PS demande d'abord une adresse IP de réseau

WAN-Man au moyen de l'adresse matérielle de ce réseau. La procédure décrite ci-dessous part du principe que le service PS a déjà obtenu une adresse IP de réseau WAN-Man:

1) le câblo-opérateur approvisionne facultativement le service PS avec des identificateurs de client uniques et spécifiques. A cette fin, il écrit des valeurs dans les entrées de l'objet cabhCdpWanDataAddrClientId de la table cabhCdpWanDataAddrTable contenue dans la base MIB du portail CDP, au moyen du fichier de configuration PS ou de message(s) SNMP de demande de mise à jour;

2) le câblo-opérateur configure le portail CDP de façon à fonctionner dans le mode 2 d'adresse de réseau WAN en écrivant une valeur différente de zéro dans l'objet cabhCdpWanDataIpAddrCount, au moyen du fichier de configuration PS ou de message(s) SNMP de demande de mise à jour;

3) une fois que le portail CDP a été configuré de façon à fonctionner dans le mode 2 d'adresse de réseau WAN décrit à l'étape 2), le service PS vérifie si des valeurs d'identificateur de client ont été approvisionnées par le système NMS comme décrit à l'étape 1). Si un nombre de valeurs d'identificateur de client supérieur ou égal à la valeur de l'objet cabhCdpWanDataIpAddrCount a été approvisionné, le service PS utilise ces valeurs dans l'option DHCP 61 au moment de la demande d'adresse(s) IP de réseau WAN-Data. Si des valeurs d'identificateur de client n'ont pas été approvisionnées, c'est-à-dire si les entrées de l'objet cabhCdpWanDataAddrClientId n'existent pas, ou si le nombre de valeurs d'identificateur de client approvisionnées est inférieur à la valeur de l'objet cabhCdpWanDataIpAddrCount, le service PS génère un nombre de valeurs uniques d'identificateur de client tel que, en combinaison avec les identificateurs de client approvisionnés, le nombre total d'identificateurs de client est égal à la valeur de l'objet cabhCdpWanDataIpAddrCount. Le service PS génère les valeurs d'identificateur de client au moyen de la seule adresse matérielle du réseau WAN-Data pour la première adresse IP de réseau WAN-Data qui a été demandée, et par concaténation de l'adresse matérielle WAN-Data avec un champ de comptage d'une longueur de 8 bits pour la deuxième adresse IP de réseau WAN-Data et pour toutes les suivantes. Si aucun identificateur de client n'a été approvisionné par le système NMS, la première valeur du champ de comptage de 8 bits est 0x02 (désignant la deuxième adresse IP de réseau WAN-Data demandée), la deuxième valeur du champ de comptage est 0x03, et ainsi de suite.

   Exemple pour le cas où aucun identificateur de client n'a été approvisionné par le système NMS:

   Adresse matérielle indiquée pour le réseau WAN-Data: 0xCDCDCDCDCDCD

   Identificateur de client généré par le service PS pour la première adresse IP de réseau WAN-Data demandée: 0xCDCDCDCDCDCD

   Identificateur de client généré par le service PS pour la deuxième adresse IP de réseau WAN-Data demandée: 0xCDCDCDCDCDCD02

   Identificateur de client généré par le service PS pour la troisième adresse IP de réseau WAN-Data demandée: 0xCDCDCDCDCDCD03

   Identificateur de client généré par le service PS pour la nième adresse IP de réseau WAN-Data demandée: 0xCDCDCDCDCDCDn (n≤0xFF)

   Si certains identificateurs de client ont été approvisionnés par le système NMS mais que leur nombre soit inférieur à la valeur de l'objet cabhCdpWanDataIpAddrCount, le service PS produit autant d'identificateurs de client additionnels que nécessaire pour rendre le nombre total d'identificateurs de client égal à la valeur de l'objet cabhCdpWanDataIpAddrCount. Le service PS génèrera ces valeurs d'identificateur de client additionnelles en adjoignant une valeur de comptage de 8 bits à l'adresse matérielle du réseau WAN-Data, en commençant par 0x02, à moins que cette valeur ne reproduise un

identificateur de client approvisionné. Si les identificateurs de client approvisionnés par le système NMS suivent le même format (adresse matérielle avec valeur de comptage de 8 bits), le service PS est tenu d'utiliser une valeur de comptage unique de façon à ne pas faire double emploi avec un identificateur de client approvisionné.

Exemple pour le cas où des identificateurs de client ont été approvisionnés par le système NMS (trois valeurs d'identificateur de client approvisionnées, cabhCdpWanDataIpAddrCount = 5):

Adresse matérielle indiquée pour le réseau WAN-Data: 0xCDCDCDCDCDCD

Premier identificateur de client approvisionné pour la première adresse IP de réseau WAN-Data: 0x0A0A0A0A0A1A

Deuxième identificateur de client approvisionné pour la deuxième adresse IP de réseau WAN-Data: 0x0A0A0A0A0A2A

Troisième identificateur de client approvisionné pour la troisième adresse IP de réseau WAN-Data: 0x0A0A0A0A0A3A

Premier identificateur de client généré par le service PS pour la quatrième adresse IP de réseau WAN-Data demandée: 0xCDCDCDCDCDCD02

Deuxième identificateur de client généré par le service PS pour la cinquième adresse IP de réseau WAN-Data demandée: 0xCDCDCDCDCDCD03

4) le service PS ajoute les valeurs d'identificateur de client qu'il généré en tant qu'entrées de l'objet cabhCdpWanDataAddrClientId jusqu'à la fin de la table cabhCdpWanDataAddrTable;

5) le service PS (client CDC) demande autant d'adresses IP uniques de réseau WAN-Data (en répétant au besoin le processus DISCOVER du protocole DHCP) que cela est spécifié par la valeur de l'objet cabhCdpWanDataIpAddrCount, au moyen de l'adresse matérielle du réseau WAN-Data contenue dans le champ *chaddr* du message DHCP et au moyen de la valeur (des valeurs) d'identificateur de client extraite(s) de l'étape 3) dans l'option DHCP 61, en commençant par la première entrée d'objet cabhCdpWanDataAddrClientId de la table cabhCdpWanDataIpAddrTable. Le client CDC n'est pas autorisé à demander plus d'adresses IP de réseau WAN-Data que cela est indiqué par la valeur de l'objet cabhCdpWanDataIpAddrCount, même si le nombre d'identificateurs de client approvisionnés est supérieur à la valeur de la table cabhCdpWanDataAddrTable.

7.2.3 Exigences relatives au portail DHCP du câble

7.2.3.1 Exigences relatives au portail CDP

Le service PS DOIT implémenter, dans ses deux configurations (imbriqué et autonome), deux adresses matérielles uniques de réseau WAN: l'adresse matérielle de réseau WAN-Man du PS et l'adresse matérielle de réseau WAN-Data du PS. La valeur numérique de l'adresse matérielle du réseau WAN-Data du PS DOIT suivre séquentiellement la valeur numérique de l'adresse matérielle du réseau WAN-Man du PS. Les adresses matérielles de réseau WAN-Man et WAN-Data du service PS DOIVENT persister après avoir été réglées en usine. Le service PS NE DOIT PAS permettre la modification de ses adresses matérielles de réseau WAN-Man et WAN-Data réglées en usine.

Dans les deux configurations du service PS (imbriqué et autonome), l'élément PS DOIT avoir des adresses matérielles d'interface avec un réseau WAN qui sont distinctes de l'adresse matérielle du câblo-modem.

7.2.3.2 Exigences relatives au serveur CDS

Le comportement du serveur CDS DOIT être conforme aux exigences du serveur figurant à la section 4.3 du document RFC 2131.

Le serveur CDS DOIT accepter l'attribution d'adresse, dynamique et manuelle, conformément à la section 1 du document RFC 2131.

L'attribution manuelle d'adresse IP par serveur CDS DOIT être prise en charge au moyen d'entrées de table cabhCdpLanAddrTable dans la base MIB du portail CDP, créées au moyen du système NMS ou du fichier de configuration PS.

Afin de prendre en charge l'attribution dynamique d'adresse IP, le serveur CDS DOIT être capable de créer, de modifier et de supprimer des entrées de table cabhCdpLanAddrTable pour les dispositifs auxquels une adresse de réseau LAN-Trans est attribuée.

Les entrées de la table de gestion des adresses de réseau LAN approvisionnées par portail CDP (table cabhCdpLanAddrTable) DOIVENT être conservées pendant une panne du câble et DOIVENT persister après un cycle d'alimentation du service PS. Le serveur CDS DOIT être en mesure de fournir des services d'adressage en protocole DHCP à des dispositifs IP de réseau LAN activés par le service PS, indépendamment de l'état de connexité du réseau WAN.

Lors d'une réinitialisation ou d'un réamorçage du service PS, le serveur CDS NE DOIT PAS, tant qu'il n'a pas été activé par le service PS, échanger de messages DHCP avec des dispositifs IP de réseau LAN.

Le service PS DOIT activer le serveur CDS, c'est-à-dire que celui-ci DOIT commencer à répondre aux messages DISCOVER et REQUEST du protocole DHCP reçus par l'intermédiaire d'une quelconque interface avec le réseau LAN du service PS, dans l'une quelconque des conditions suivantes (voir également la Figure 13-2):

- lorsque le service PS fonctionne en mode d'approvisionnement DHCP, après que le client CDC a reçu une location d'adresse IP de réseau WAN-Man de services PS et après que le service PS a reçu et traité correctement un fichier de configuration PS;
- lorsque le service PS fonctionne en mode d'approvisionnement SNMP, après que le client CDC a reçu une location d'adresse IP de réseau WAN-Man de services PS, qu'il s'est authentifié auprès du serveur du centre de distribution de clés (KDC, *key distribution centre*) et qu'il s'est correctement inscrit auprès du système NMS;
- lorsque la première tentative du client CDC d'acquérir une adresse IP de réseau WAN-Man du service PS échoue;
- lorsque le service PS fonctionne en mode d'approvisionnement DHCP et que la première tentative de téléchargement ou de traitement du fichier de configuration PS échoue;
- lorsque le service PS fonctionne en mode d'approvisionnement SNMP et que la première tentative d'authentification auprès du serveur de centre KDC échoue;
- lorsque le service PS fonctionne en mode d'approvisionnement SNMP et est appelé à télécharger un fichier de configuration PS avant que le fonctionnement du serveur CDS soit lancé, et que la première tentative de téléchargement ou de traitement du fichier de configuration PS échoue.

Le serveur CDS DOIT attribuer – à chaque dispositif IP de réseau LAN contenu dans le secteur LAN-Trans qui demande une adresse IP par protocole DHCP – une adresse IP unique, extraite de la réserve d'adresses commençant par l'objet cabhCdpLanPoolStart et se terminant par l'objet cabhCdpLanPoolEnd si le nombre d'adresses déjà attribuées par ce serveur CDS est inférieur à la valeur de l'objet cabhCdpLanTransThreshold.

Si la valeur de l'objet cabhCdpLanTransThreshold est 0, le serveur CDS DOIT traiter le seuil comme s'il avait été affecté de la plus grande valeur possible afin de désigner la taille actuelle de la réserve d'adresses IP de réseau LAN-Trans (définie par les valeurs de début (cabhCdpLanPoolStart) et de fin (cabhCdpLanPoolEnd) de réserve d'adresses IP de réseau LAN-Trans).

Le serveur CDS DOIT maintenir le paramètre de compte d'adresses (objet cabhCdpLanTransCurCount) indiquant le nombre de locations d'adresse de réseau LAN-Trans accordées à des dispositifs IP de réseau LAN.

Le compte d'adresses DOIT augmenter chaque fois qu'une location d'adresse LAN-Trans est accordée à un dispositif IP de réseau LAN et DOIT diminuer chaque fois qu'une adresse LAN-Trans est libérée ou qu'une location d'adresse LAN-Trans arrive à expiration.

Le serveur CDS DOIT comparer le paramètre de compte d'adresses (cabhCdpLanTransCurCount) au paramètre de seuil d'adresses (cabhCdpLanTransThreshold) après l'attribution d'une adresse de réseau LAN-Trans. Si le paramètre de compte d'adresses (cabhCdpLanTransCurCount) dépasse le paramètre de seuil d'adresses (cabhCdpLanTransThreshold), une notification DOIT être générée conformément au mécanisme de rapport d'événement défini au § 6.5 et à l'Annexe B. Pendant que le paramètre de compte d'adresses (cabhCdpLanTransCurCount) dépasse le paramètre de seuil d'adresses (cabhCdpLanTransThreshold), le serveur CDS DOIT être capable d'effectuer les actions suivantes sur dépassement de seuil en réponse au prochain message DISCOVER émis par le réseau LAN en protocole DHCP: attribuer une adresse LAN-Trans selon la procédure normale ou ne pas attribuer d'adresse.

Si l'objet cabhCdpLanTransCurCount a une valeur égale ou supérieure à celle de l'objet cabhCdpLanTransThreshold ET si un dispositif IP de réseau LAN demande une location d'adresse IP supplémentaire, l'action spécifiquement effectuée par le serveur CDS DOIT être conforme à l'indication donnée par le paramètre d'action sur dépassement de seuil (cabhCdpLanTransAction) qui a été approvisionné.

Le serveur CDS ne DOIT attribuer des adresses IP et acheminer les paramètres de configuration DHCP, énumérés dans le Tableau 7-3 et pour lesquels le serveur CDS possède une valeur valide, qu'à des dispositifs IP de réseau LAN recevant une adresse dans le secteur d'adresses LAN-Trans.

Si le câblo-opérateur approvisionne des valeurs pour une rangée de la table cabhCdpLanAddrTable, le service PS (serveur CDS) DOIT offrir, au dispositif IP de réseau LAN dont l'adresse matérielle correspond à l'identificateur cabhCdpLanAddrClientID approvisionné, une location relative à l'adresse IP cabhCdpLanAddrIp approvisionnée, en réponse à un message DHCP DISCOVER reçu de ce dispositif IP de réseau LAN.

Lorsque le serveur CDS attribue à un dispositif IP de réseau LAN une location active pour une adresse IP, le portail CDP DOIT supprimer cette adresse de la réserve d'adresses IP disponibles pour attribution à des dispositifs IP de réseau LAN.

Si le serveur CDS reçoit, d'un dispositif IP de réseau LAN, une demande de location qu'il ne peut pas satisfaire en raison de la non-disponibilité d'adresses dans la réserve d'adresses IP (définie par les objets cabhCdpLanPoolStart et cabhCdpLanPoolEnd), il doit signaler cet événement conformément à l'Annexe B et au mécanisme de rapport d'événement défini au § 6.5.

Le serveur CDS DOIT mémoriser la valeur transmise dans le champ *chaddr* du message de demande DHCP envoyé par le dispositif IP de réseau LAN lorsqu'une location active est créée pour ce dispositif IP de réseau LAN.

Le service PS DOIT prendre en charge tous les objets de base MIB de portail CDP IPCable2Home, y compris tous les objets contenus dans la table cabhCdpLanAddrTable, les objets cabhCdpLanPool, les objets cabhCdpServer et les objets cabhCdpLanTrans.

Le serveur CDS DOIT prendre en charge les options DHCP indiquées comme étant obligatoires dans la colonne relative à la prise en charge du protocole CDS du Tableau 7-3.

Le serveur CDS DOIT prendre en charge l'offre des valeurs par défaut indiquées dans la colonne du Tableau 7-3 relative aux valeurs par défaut d'usine de serveur CDS, si l'option DHCP n'a pas été approvisionnée avec d'autres valeurs.

Si le mode de traitement primaire de paquet PS (objet cabhCapPrimaryMode) a été mis à la valeur "traversée" ET si le processus d'approvisionnement du service PS a été effectué (comme indiqué par l'objet cabhPsDevProvState = pass(1)), alors le serveur CDS DOIT être désactivé.

Le serveur CDS NE DOIT PAS répondre aux messages DHCP qui sont reçus par l'intermédiaire d'une quelconque interface avec un réseau WAN, ni émettre de messages DHCP à partir d'une quelconque interface avec un réseau WAN.

Le serveur CDS NE DOIT PAS acheminer d'option DHCP de valeur néant vers un quelconque dispositif IP de réseau LAN.

Tableau 7-3/J.191 – Options DHCP de serveur CDS

Numéro d'option	Fonction de l'option	Prise en charge du protocole CDS: (O)bligatoire (F)acultative	Valeurs par défaut d'usine de serveur CDS	Nom d'objet MIB
0	Bourrage	O	N/A	N/A
255	Fin	O	N/A	N/A
1	Gabarit de sous-réseau	O	255.255.255.0	cabhCdpServerSubnetMask
2	Décalage temporel	O	0	cabhCdpServerTimeOffset
3	Option de routeur	O	192.168.0.1	cabhCdpServerRouter
6	Serveur de nom de domaine	O	192.168.0.1	cabhCdpServerDnsAddress
7	Serveur d'enregistrement	O	0.0.0.0	cabhCdpServerSyslogAddress
12	Nom de serveur	O	N/A	N/A
15	Nom de Domaine	O	Chaîne vide	cabhCdpServerDomainName
23	Temps de recherche de relais	O	64	cabhCdpServerTTL
26	Unité MTU d'interface	O	N/A	cabhCdpServerInterfaceMTU
43	Informations spécifiques du vendeur	O	Choisies par le vendeur	cabhCdpServerVendorSpecific
50	Adresse IP demandée	O	N/A	N/A
51	Temps de location d'adresse IP	O	3600 secondes	cabhCdpServerLeaseTime
54	Identificateur de serveur	O	192.168.0.1	cabhCdpServerDhcpAddress
55	Liste de demande de paramètres	O	N/A	N/A
60	Identificateur de classe de vendeur	O	N/A	N/A

7.2.3.3 Exigences relatives au client CDC

Le comportement du client CDC DOIT être conforme aux exigences de client indiquées dans le document RFC 2131.

Le service PS DOIT diffuser le message DHCP DISCOVER conformément aux exigences de client indiquées dans le document RFC 2131, et tenter d'acquérir un prêt d'adresse IP de réseau WAN-Man de service PS pendant le processus d'initialisation du service PS.

Le service PS DOIT mettre l'objet cabhPsDevProvState à la valeur inProgress(2) lorsque le service PS diffuse le message DHCP DISCOVER pour la première fois après un réamorçage du dispositif ou une réinitialisation du service PS.

Le comportement d'approvisionnement complet du service PS est défini dans le Tableau 13-1 pour le mode d'approvisionnement DHCP et dans le Tableau 13-2 pour le mode d'approvisionnement SNMP.

Le client CDC DOIT utiliser l'adresse matérielle de réseau WAN-Man du service PS contenue dans le champ *chaddr* ET dans l'option DHCP 61 ainsi que dans les messages DHCP DISCOVER et REQUEST lors d'une demande d'adresse IP de réseau WAN-Man auprès du serveur DHCP de tête de réseau.

Si la valeur de l'objet cabhCdpWanDataIpAddrCount est zéro, le service PS DOIT utiliser l'adresse IP du réseau WAN-Man pour les interfaces avec les réseaux WAN-Man et WAN-Data.

Si la valeur de l'objet cabhCdpWanDataIpAddrCount est supérieure à zéro, le service PS DOIT demander le même nombre d'adresse(s) IP unique(s) de réseau WAN-Data auprès du serveur DHCP de tête de réseau, en tant que valeur de l'objet cabhCdpWanDataIpAddrCount.

Le service PS (client CDC) NE DOIT PAS tenter d'acquérir plus d'adresses IP de réseau WAN-Data que la valeur de l'objet cabhCdpWanDataIpAddrCount.

Le client CDC DOIT utiliser un identificateur cabhCdpWanDataAddrClientId dans l'option DHCP 61 pour chaque adresse IP de réseau WAN-Data demandée au serveur DHCP de tête de réseau.

Le client CDC DOIT utiliser l'adresse matérielle du réseau WAN-Data comme valeur contenue dans le champ *chaddr* pour chaque adresse IP de réseau WAN-Data demandée au serveur DHCP de tête de réseau.

Lorsque le client CDC demande au serveur DHCP de tête de réseau des adresses IP de réseau WAN-Data, ce serveur DOIT utiliser les entrées d'identificateur cabhCdpWanDataAddrClientId pour l'option DHCP 61, dans l'ordre d'apparition de ces entrées dans la table cabhCdpWanDataAddrTable, en commençant par la première entrée.

Si une valeur différente de zéro est configurée pour l'objet cabhCdpWanDataIpAddrCount et si le nombre d'entrées d'identificateur cabhCdpWanDataAddrClientId est inférieur à la valeur de l'objet cabhCdpWanDataIpAddrCount, le service PS DOIT générer autant d'identificateurs de client de réseau WAN-Data uniques que nécessaire pour que le nombre total d'entrées d'identificateur cabhCdpWanDataAddrClientId soit égal à la valeur de l'objet cabhCdpWanDataIpAddrCount et DOIT ajouter chaque entrée ainsi générée à la fin de la table cabhCdpWanDataAddrTable.

Si le service PS génère des identificateurs de client de réseau WAN-Data, la première entrée d'identificateur cabhCdpWanDataAddrClientId de la table cabhCdpWanDataAddrTable DOIT être l'adresse matérielle du réseau WAN-Data.

Si le service PS génère des identificateurs de client de réseau WAN-Data, toute entrée d'identificateur cabhCdpWanDataAddrClientId générée par le service PS, autre que la première entrée de la table cabhCdpWanDataAddrTable, DOIT être l'adresse matérielle du réseau WAN-Data assortie d'une valeur finale de comptage sur 8 bits commençant par 0x02, à moins que cette valeur n'existe déjà en tant qu'entrée d'identificateur cabhCdpWanDataAddrClientId auquel cas le service PS DOIT produire l'identificateur de client sous la forme de l'adresse matérielle du réseau WAN-Data assortie de la prochaine valeur disponible de comptage sur 8 bits.

Le service PS DOIT implémenter l'option d'informations spécifiques du vendeur (option DHCP 43) comme spécifié dans les Tableaux 7-5 et 7-6. Les détails de l'option DHCP 43 et de ses sous-options pour l'environnement CableHome 1.0 sont mieux définis ci-dessous. Les définitions des sous-options de l'option DHCP 43 DOIVENT être conformes aux exigences imposées par le document RFC 2132.

L'option commence par un octet de type ayant la valeur numérique 43, suivi par un octet de longueur, lui-même suivi par un nombre d'octets de données égal à la valeur de l'octet de longueur. La valeur de l'octet de longueur ne comprend pas les deux octets qui spécifient la balise et la longueur.

L'option DHCP 43 de l'environnement CableHome 1.0 est de nature composite car son contenu se subdivise en une ou plusieurs sous-options. Les sous-options de l'option DHCP 43 prises en charge dans l'environnement CableHome 1.0 sont les suivantes: 1, 2, 3, 4, 5, 6, 11, 12, 13 et 14. Une sous-option commence par un octet de balise contenant le code de sous-option, suivi d'un octet de longueur qui indique le nombre total d'octets de données. La valeur de l'octet de longueur ne comprend pas cet octet proprement dit ni l'octet de balise. L'octet de longueur est suivi des octets "de longueur" des données de sous-option.

Le codage de chaque sous-option de l'option DHCP 43 est défini ci-dessous. Voir dans les Tableaux 7-5 et 7-6 la finalité prévue de chaque sous-option.

Le service PS DOIT coder la sous-option 1 de l'option DHCP 43 par le nombre d'octets qui est égal à la valeur de l'octet de longueur de cette sous-option, chaque octet codifiant une sous-option demandée.

Le service PS DOIT coder chacune des sous-options 2, 3, 4, 5, 6, 12, 13 et 14 de l'option DHCP 43 sous la forme d'une chaîne de caractères extraits du jeu de caractères ASCII de terminal NVT, sans caractère NULL final.

Un service PS autonome DOIT envoyer la sous-option 2 de l'option DHCP 43 contenant la chaîne de caractères "SPS" (sans les guillemets).

Un service PS imbriqué DOIT envoyer la sous-option 2 de l'option DHCP 43 contenant la chaîne de caractères "EPS" (sans les guillemets).

Un service PS autonome DOIT envoyer la sous-option 3 de l'option DHCP 43 contenant la chaîne de caractères "SPS" (sans les guillemets).

Un service PS imbriqué DOIT envoyer la sous-option 3 de l'option DHCP 43 contenant une liste à séparation par deux points de tous les types de dispositif contenus dans le dispositif complet, y compris au minimum la chaîne de caractères "ECM:EPS" (sans les guillemets).

Si le service PS demande une location d'adresse IP de réseau WAN-Man, il DOIT envoyer la sous-option 11 de l'option DHCP 43 contenant la valeur 0x01, codée en nombre binaire, dans ses messages DHCP DISCOVER et REQUEST.

Si le service PS demande une location d'adresse IP de réseau WAN-Data, il DOIT envoyer la sous-option 11 de l'option DHCP 43 contenant la valeur 0x02, codée en nombre binaire, dans ses messages DHCP DISCOVER et REQUEST.

Le Tableau 7-4 résume la façon dont le service PS est tenu de régler les valeurs de la sous-option 11 de l'option DHCP 43 pour les interfaces du service PS avec le réseau WAN.

La limite de longueur des sous-options 4, 5, 6, 12, 13 et 14 est de 255 octets chacune. La longueur totale de l'option DHCP 43 pourrait donc dépasser 255 octets. Si le nombre total d'octets contenus dans toutes les sous-options de l'option DHCP 43 dépasse 255 octets, le service PS DOIT se conformer au document RFC 3396 afin de subdiviser l'option en de multiples options plus petites.

Le client CDC DOIT implémenter l'option d'identificateur de classe du vendeur (l'option DHCP 60) comme spécifié dans les Tableaux 7-5 et 7-6.

Tableau 7-4/J.191 – Valeurs de la sous-option 11 de l'option DHCP 43

Identificateur d'élément	Description et commentaires
PS WAN-Man = 0x01	Identifie la demande d'adresse de secteur WAN-Man
PS WAN-Data = 0x02	Identifie la demande d'adresse de secteur WAN-Data

Dans le cas d'un service PS imbriqué avec un câblo-modem, celui-ci et l'élément de services PS envoient chacun des demandes DHCP séparées. Le Tableau 7-5 décrit comment le client CDC DOIT régler le contenu des options 60 et 43 pour le service portail lorsque l'élément de services PS est imbriqué avec un câblo-modem et que des adresses séparées de gestion de réseau WAN de PS et de réseau WAN-Data de PS sont demandées.

Tableau 7-5/J.191 – Options DHCP des demandes d'adresse de réseau WAN-Man et WAN-Data pour services PS imbriqués

Options de demande DHCP	Valeur	Description
Demande DHCP d'adresse de réseau WAN-Man pour services portail imbriqués		
Option d'équipement CPE 60	"IPCable2Home"	
Option d'équipement CPE 43 sous-option 1	Demander un vecteur de sous-option	Liste des sous-options (dans l'option 43) à renvoyer par le serveur. Aucune n'est définie.
Option d'équipement CPE 43 sous-option 2	"EPS"	Service PS imbriqué
Option d'équipement CPE 43 sous-option 3	"ECM:EPS"	Liste des dispositifs imbriqués (CM imbriqué et PS imbriqué)
Option d'équipement CPE 43 sous-option 4	Par exemple, "123456"	Numéro de série du CM/PS
Option d'équipement CPE 43 sous-option 5	Par exemple, "v3.2.1"	Numéro de version matérielle du dispositif CM/PS
Option d'équipement CPE 43 sous-option 6	Par exemple, "v1.0.2"	Numéro de version logicielle du dispositif CM/PS
Option d'équipement CPE 43 – sous-option 11	PS WAN-Man (0x01)	Définit qu'une adresse est demandée dans le secteur WAN-Man des services PS
Option d'équipement CPE 43 sous-option 12	Par exemple, "ABC s.a. CM-PS123…"	Description du système CM/PS d'après l'objet sysDescr
Option d'équipement CPE 43 sous-option 13	Par exemple, "CM-PS123-1.02…"	Révision de la micrologique de CM/PS d'après l'objet docsDevSwCurrentVers
Option d'équipement CPE 43 sous-option 14	Par exemple, "1.2.3…"	Version du fichier de politique de pare-feu d'après l'objet cabhSecFwPolicyFileCurrent-Version

Tableau 7-5/J.191 – Options DHCP des demandes d'adresse de réseau WAN-Man et WAN-Data pour services PS imbriqués

Options de demande DHCP	Valeur	Description
Demande DHCP d'adresse de réseau WAN-Data pour services portail imbriqués		
Option d'équipement CPE 60	"IPCable2Home"	
Option d'équipement CPE 43 – sous-option 1	Demander un vecteur de sous-option	Liste des sous-options (dans l'option 43) à renvoyer par le serveur. Aucune n'est définie.
Option d'équipement CPE 43 – sous-option 2	"EPS"	Service PS imbriqué
Option d'équipement CPE 43 – sous-option 3	"ECM:EPS"	Liste des dispositifs imbriqués (CM imbriqué et PS imbriqué)
Option d'équipement CPE 43 – sous-option 4	Par exemple, "123456"	Numéro de série de dispositif CM/PS
Option d'équipement CPE 43 – sous-option 11	WAN-Data de PS (0x02)	Définit qu'une adresse est demandée dans le secteur WAN-Data des services PS

Le Tableau 7-6 décrit le réglage que le client CDC DOIT effectuer dans le contenu des options 60 et 43, lorsque le service PS est un dispositif autonome.

Tableau 7-6/J.191 – Options DHCP des demandes d'adresse de réseau WAN-Man et WAN-Data pour services PS autonomes

Options de demande DHCP	Valeur	Description
Demande DHCP d'adresse de réseau WAN-Man pour services portail autonomes		
Option d'équipement CPE 60	"IPCable2Home"	
Option d'équipement CPE 43 sous-option 1	Demander un vecteur de sous-option	Liste des sous-options (dans l'option 43) à renvoyer par le serveur. Aucune n'est définie.
Option d'équipement CPE 43 sous-option 2	"SPS"	Service PS autonome
Option d'équipement CPE 43 sous-option 3	"SPS"	Liste des dispositifs imbriqués (PS autonome seulement)
Option d'équipement CPE 43 sous-option 4	Par exemple, "123456"	Numéro de série du dispositif de services PS
Option d'équipement CPE 43 sous-option 5	Par exemple, "v3.2.1"	Numéro de version matérielle du dispositif PS
Option d'équipement CPE 43 sous-option 6	Par exemple, "v1.0.2"	Numéro de version logicielle du dispositif PS
Option d'équipement CPE 43 – sous-option 11	PS WAN-Man (0x01)	Définit qu'une adresse est demandée dans le secteur WAN-Man des services PS
Option d'équipement CPE 43 sous-option 12	Par exemple, "ABC s.a. PS123…"	Description du système PS d'après l'objet sysDescr

Tableau 7-6/J.191 – Options DHCP des demandes d'adresse de réseau WAN-Man et WAN-Data pour services PS autonomes

Options de demande DHCP	Valeur	Description
Option d'équipement CPE 43 sous-option 13	Par exemple, "PS123-1.02…"	Révision de la micrologique de services PS d'après l'objet docsDevSwCurrentVers
Option d'équipement CPE 43 sous-option 14	Par exemple, "1.2.3…"	Version du fichier de politique de pare-feu d'après l'objet cabhSecFwPolicyFileCurrent-Version
Demande DHCP d'adresse de réseau WAN-Data pour services portail autonomes		
Option d'équipement CPE 60	"IPCable2Home"	
Option d'équipement CPE 43 – sous-option 1	Demander un vecteur de sous-option	Liste des sous-options (dans l'option 43) à renvoyer par le serveur. Aucune n'est définie.
Option d'équipement CPE 43 – sous-option 2	"SPS"	Service PS autonome
Option d'équipement CPE 43 – sous-option 3	"SPS"	Liste des dispositifs imbriqués (service PS autonome seulement)
Option d'équipement CPE 43 – sous-option 4	Par exemple, "123456"	Numéro de série du dispositif de services PS
Option d'équipement CPE 43 – sous-option 11	WAN-Data de PS (0x02)	Définit qu'une adresse est demandée dans le secteur WAN-Data des services PS

Une description détaillée du contenu de l'objet sysDescr des services PS figure dans le § 6.3.4.

Le service PS DOIT accepter les options DHCP indiquées comme obligatoires dans la colonne *Prise en charge du protocole CDC* du Tableau 7-7 ci-dessous, qui énumère les options DHCP dont la prise en charge par le client CDC est obligatoire ou facultative.

Tableau 7-7/J.191 – Options DHCP de client CDC

Numéro d'option	Fonction de l'option	Prise en charge du protocole CDC (O)bligatoire
0	Bourrage	O
255	Fin	O
1	Gabarit de sous-réseau	O
2	Option de décalage horaire	O
3	Option de routeur	O
4	Option de serveur temporel	O
6	Serveur de nom de domaine	O
7	Serveur d'enregistrement (syslog)	O
12	Nom de serveur	O
15	Nom de domaine	O

Tableau 7-7/J.191 – Options DHCP de client CDC

Numéro d'option	Fonction de l'option	Prise en charge du protocole CDC (O)bligatoire
23	Temps par défaut de recherche de relais	O
26	Unité MTU d'interface	O
43	Informations spécifiques du vendeur	O
50	Adresse IP demandée	O
51	Heure de location d'adresse IP	O
54	Identificateur de serveur	O
55	Liste de demande de paramètre	O
60	Identificateur de classe de vendeur	O
61	Identificateur de client	O
177	Sous-option 3 – Adresse d'entité SNMP du fournisseur de services	O
177	Sous-option 6 – Nom du secteur Kerberos du secteur d'approvisionnement	O
177	Sous-option 51 – Adresse IP de serveur Kerberos	O

Le service portail DOIT accepter une adresse d'entité SNMP de fournisseur de services (option DHCP 177, sous-option 3) configurée comme une adresse IPv4. Le format de la sous-option 3 de l'option DHCP 177 est décrit ci-dessous:

La longueur de la sous-option 3 de l'option DHCP 177 DOIT être de 5 octets. L'octet de longueur de la sous-option 3 de l'option DHCP 177 DOIT être suivi d'un seul octet qui indique le type d'adresse spécifique qui suit. La valeur de l'octet "type d'adresse" de la sous-option 3 de l'option DHCP 177 DOIT être mise à 1 afin d'indiquer une adresse IPv4. L'octet "type d'adresse" de la sous-option 3 de l'option DHCP 177 DOIT être suivi de 4 octets d'adresse IPv4.

Le service PS DOIT ignorer la sous-option 3 de l'option DHCP 177 si son format ou son contenu n'est pas conforme aux exigences de cette sous-option.

Code	Longueur	Type	Adresse			
3	5	1	a1	a2	a3	a4

Le service PS DOIT prendre en charge un nom de secteur Kerberos (sous-option 6 de l'option DHCP 177). Un nom de secteur Kerberos est requis par le service PS afin d'autoriser une exploration par service DNS en vue de trouver l'adresse de l'entité de centre de distribution de clés (KDC) du fournisseur de services. Le format de la sous-option 6 de l'option DHCP 177 est décrit ci-dessous:

Le nom du secteur Kerberos fourni au service PS dans la sous-option 6 de l'option DHCP 177 DOIT être codé en fonction du nom de secteur de style domanial décrit dans le document RFC 1510. Le nom de secteur Kerberos fourni au service PS dans la sous-option 6 de l'option DHCP 177 DOIT être écrit entièrement en lettres majuscules et être conforme à la syntaxe décrite dans la section 3.1 du document RFC 1035. La sous-option est codée comme suit:

Code	Longueur	Nom du secteur Kerberos			
6	n	k1	k2	…	kn

Le service PS DOIT ignorer la sous-option 6 de l'option DHCP 177 si son format ou son contenu n'est pas conforme aux exigences pour cette sous-option.

Le service PS DOIT prendre en charge une adresse IP de serveur Kerberos (sous-option 51 de l'option DHCP 177). La sous-option d'adresse IP de serveur Kerberos informe le service PS de l'adresse dans le réseau d'un ou de plusieurs serveurs de centre de distribution de clés.

Le codage de la sous-option d'adresse de serveur de centre KDC sera conforme au format d'une adresse IPv4 utilisant le point d'accès par défaut. La longueur minimale de la sous-option 51 de l'option DHCP 177 est de 4 octets et cette longueur DOIT toujours être un multiple de 4. Si de multiples serveurs de centre KDC sont énumérés dans la sous-option 51 de l'option DHCP 177, ces serveurs DOIVENT être énumérés en ordre de priorité décroissante. La sous-option d'adresse de serveur de centre KDC est codée comme suit:

Code	**Longueur**	**Adresse 1**				**Adresse 2**		
51	N	a1	a2	a3	a4	a1	a2	…

Le service PS DOIT essayer d'effectuer des échanges de clés avec les centres KDC dans l'ordre de la liste contenue dans la sous-option 51 de l'option DHCP 177, jusqu'à ce que l'échange de clés ait réussi avec un des centres KDC ou jusqu'à ce que la liste soit épuisée et que les échanges de clés échouent. Voir au § 11.3.1 les exigences relatives à l'échange de clés dans le service PS. Celui-ci DOIT ignorer la sous-option 51 de l'option DHCP 177 si son format ou son contenu n'est pas conforme aux exigences de cette sous-option.

Le service PS DOIT inclure, dans les messages DHCP DISCOVER et REQUEST envoyés au serveur DHCP du réseau câblé, les options DHCP énumérées dans le Tableau 7-8 comme étant obligatoires.

Tableau 7-8/J.191 – Options DHCP de client CDC contenues dans les messages DISCOVER et REQUEST

Numéro d'option	**Fonction d'option**	**Inclusion du protocole CDC (O)bligatoire**
255	Fin	O
43	Informations spécifiques du vendeur	O
50	Adresse IP demandée	O
55	Liste de demande de paramètre	O
60	Identificateur de classe de vendeur	O
61	Identificateur de client	O

Le service PS DOIT demander les options DHCP énumérées comme étant obligatoires dans le Tableau 7-9, dans le cadre de l'option DHCP 55 (Liste de demande de paramètres) [RFC 2132] envoyée dans les messages DHCP DISCOVER et REQUEST.

Tableau 7-9/J.191 – Options DHCP de client CDC demandées dans le cadre de l'option 55

Numéro d'option	Fonction d'option	Inclusion du protocole CDC (O)bligatoire
1	Masque de sous-réseau	O
2	Option de décalage temporel	O
3	Option de routeur	O
4	Option de serveur temporel	O
6	Serveur de nom de domaine	O
7	Serveur d'enregistrement (syslog)	O
15	Nom de domaine	O
23	Temps par défaut de recherche de relais	O
26	Unité MTU d'interface	O
51	Temps de location d'adresse IP	O
54	Identificateur de serveur	O
177	Option de configuration de client compatible avec PacketCa	O

Chaque fois que la première interface PS/WAN-Data n'a pas de location DHCP en cours, cette première interface PS/WAN-Data DOIT avoir par défaut les paramètres IP suivants:

- Adresse IP "de repli" du réseau WAN-Data: 192.168.100.5
- Masque de réseau: 255.255.255.0
- Passerelle par défaut: 192.168.100.1

La finalité de l'adresse IP "de repli" d'un réseau WAN-Data est de permettre l'accès à l'adresse IP de diagnostic du câblo-modem (192.168.100.1) à partir d'un dispositif IP de réseau LAN. L'adresse IP "de repli" d'un réseau WAN-Data NE DOIT être utilisée que comme partie d'adresse IP de réseau WAN du champ de traduction dynamique NAT ou NAPT d'un mappage de traduction d'adresse C-NAT ou C-NAPT, selon le cas. Si le service PS fonctionne en mode 2 d'adresse de réseau WAN et est tenu d'essayer d'acquérir de multiples locations d'adresse IP de réseau WAN-Data ET si le service PS n'est pas en mesure d'acquérir ces locations après avoir émis trois messages DHCP DISCOVER (conformément aux procédures DHCP de réessai spécifiées au § 7.2.3.3), le service PS DOIT utiliser l'adresse IP "de repli" de réseau WAN-Data en tant que partie WAN de chaque champ de traduction dynamique NAT, jusqu'à ce que le service PS obtienne la ou les locations nécessaires d'adresse IP de réseau WAN-Data auprès d'un serveur DHCP par l'intermédiaire d'une interface PS/WAN.

L'adresse IP "de repli" d'un réseau WAN-Data NE DOIT pas être utilisée lorsque le service PS est configuré de façon à fonctionner dans le mode de traitement primaire de paquet de type traversée.

Le service PS NE DOIT PAS utiliser l'adresse IP "de repli" d'un réseau WAN-Data pour de quelconques mappages de traduction C-NAT ou C-NAPT lorsque le service PS possède une location actuelle d'adresse IP de réseau WAN-Man et WAN-Data. Si un serveur DHCP offre à l'interface PS/WAN une location au service PS (client CDC) pour l'adresse IP 192.168.100.5, c'est-à-dire la même adresse que l'adresse IP "de repli" d'un réseau WAN-Data, le service PS (client CDC) PEUT accepter cette location et utiliser cette adresse en tant qu'adresse IP "de repli" d'un réseau WAN-Data pour un mappage de traduction C-NAT ou C-NAPT.

Même en utilisant l'adresse IP de réseau WAN-Data par défaut 192.168.100.5, le client CDC DOIT continuer à émettre un message DHCP DISCOVER toutes les 10 s jusqu'à ce qu'une location DHCP

valide soit accordée à cette interface WAN-Data/PS (ou à l'interface avec le réseau WAN-Man si le réseau WAN-Man et le réseau WAN-data partagent une seule adresse IP).

Lorsqu'un service portail acquiert une adresse IP de gestion de réseau WAN pour son interface WAN-Man, le client CDC DOIT toujours insérer son adresse matérielle de réseau WAN dans le champ d'identificateur de client (option DHCP 61) du message DHCP DISCOVER.

Si, lors de sa tentative d'acquérir une location pour l'adresse IP de réseau WAN-Man du service PS, le client CDC ne reçoit aucun message DHCP OFFER, le service PS DOIT enregistrer l'identificateur d'événement ID 68000100 dans le journal local et rediffuser un message DHCP DISCOVER (c'est-à-dire relancer la séquence d'approvisionnement si cette condition d'échec apparaît) en répétant jusqu'à 5 fois cette tentative d'acquisition de location DHCP. Si le client CDC, lors de sa cinquième tentative d'acquisition d'une location d'adresse IP de réseau WAN-Man du service PS, ne reçoit aucun message DHCP OFFER, le service PS DOIT utiliser l'adresse IP "de repli" de réseau WAN, le masque de réseau et la passerelle par défaut comme décrit ci-dessus ET continuer à essayer d'obtenir une adresse IP valide de réseau WAN-Man en diffusant toutes les 10 s le message DHCP DISCOVER à partir de son interface avec le réseau WAN jusqu'à ce qu'une location DHCP valide soit accordée pour l'adresse IP du réseau WAN-Man.

Si le client CDC reçoit, au cours du processus d'acquisition d'une location pour l'adresse IP de réseau WAN-Man du service PS, une adresse IP valide contenue dans le champ 'siaddr' du message DHCP ACK [RFC 2131] reçu du serveur DHCP dans le réseau câblé ET un nom de fichier valide dans le champ 'file' ET ne reçoit pas la sous-option 3, la sous-option 6 OU la sous-option 51 (combinaison valide 1) de l'option DHCP 177, le service PS DOIT mettre l'objet cabhPsDevProvMode à la valeur '1' (mode d'approvisionnement DHCP) et essayer de synchroniser l'heure actuelle avec le serveur temporel ToD comme décrit au § 7.4.3.

Si, au cours du processus d'acquisition d'une location pour l'adresse IP de réseau WAN-Man du service PS, le client CDC reçoit un message DHCP ACK du serveur DHCP dans le réseau câblé contenant l'option DHCP 177 avec une adresse IP valide (adresse d'entité SNMP) dans la sous-option 3, un nom de secteur Kerberos valide dans la sous-option 6 ET une adresse IP valide (adresse IP de serveur Kerberos) dans la sous-option 51 ET ne reçoit pas d'adresse IP valide dans le champ 'siaddr' ET ne reçoit pas de nom de fichier valide dans le champ 'file' (combinaison valide 2), le service PS DOIT mettre l'objet cabhPsDevProvMode à la valeur '2' (mode d'approvisionnement SNMP) ET DOIT mettre en fonctionnement le serveur CDS ET DOIT essayer de synchroniser l'heure actuelle avec le serveur temporel ToD et se légitimer auprès du serveur de centre KDC comme décrit dans le § 11.

Si le client CDC reçoit, au cours du processus d'acquisition d'une location pour l'adresse IP de réseau WAN-Man du service PS, dans le message DHCP ACK reçu du serveur DHCP dans le réseau câblé, une combinaison quelconque des sous-options 3, 6 et 51 de l'option DHCP 177, d'un champ 'siaddr' et d'un champ 'file' autre que les deux combinaisons valides décrites ci-dessus, le service PS a reçu une configuration DHCP non valide et DOIT enregistrer l'événement approprié et rediffuser un message DHCP DISCOVER (c'est-à-dire relancer la séquence d'approvisionnement en présence de cette condition non valide) en répétant jusqu'à 5 fois l'ensemble du processus d'acquisition de location DHCP.

Si, lors de sa cinquième tentative d'acquisition d'une location pour l'adresse IP de réseau WAN-Man du service PS, le client CDC reçoit, dans le message DHCP ACK reçu du serveur DHCP dans le réseau câblé, une combinaison quelconque des sous-options 3, 6 et 51 de l'option DHCP 177, d'un champ 'siaddr' et d'un champ 'file' autre que les deux combinaisons valides décrites ci-dessus, le service PS DOIT effectuer les opérations suivantes dans l'hypothèse qu'il est connecté au moyen d'un câblo-modem à un réseau de transmission de données par câble qui ne prend pas en charge l'approvisionnement CableHome (mode CableHome inactif):

- désactiver l'agent SNMP (portail CMP) pour l'accès à l'interface avec le réseau WAN; Laisser l'agent SNMP activé pour les messages reçus par l'intermédiaire de l'interface avec le réseau LAN (c'est-à-dire pour les messages SNMP adressés au routeur-serveur du service PS);
- désactiver le client du protocole TFTP;
- désactiver le rapport d'événement SYSLOG;
- accepter la location d'adresse IP offerte (équipement CPE) et l'utiliser comme adresse de réseau WAN-Data du service PS dans la table de mappage du portail CAP, y compris l'attribution de cette adresse à l'objet cabhCdpWanDataAddrIp et l'insertion des autres entrées de la table d'adresses IP de réseau WAN-Data du portail CDP (objet cabhCdpWanDataAddrTable). Le service PS fonctionnera sans adresse IP de réseau WAN-Man, ce qui est différent de chacun des modes d'adresse de réseau WAN décrits au § 7.2.2.2.2;
- arrêter le temporisateur d'approvisionnement;
- mettre la valeur de l'objet cabhPsDevProvMode à "dormantCHmode(3)";
- mettre la valeur de l'objet cabhPsDevProvState à "fail(3)";
- activer le serveur CDS;
- activer le portail CAP et la fonctionnalité de commutation USFS;
- active le portail CNP;
- activer le pare-feu;
- fonctionner avec les paramètres qui ont déjà été approvisionnés, y compris ceux qui ont été extraits des valeurs d'objets persistants de base MIB. Le service PS fonctionnant en mode CableHome inactif NE DOIT PAS réinitialiser ses objets de base MIB aux réglages par défaut d'usine.

Lorsqu'un service portail fonctionnant en mode 2 d'adresse de réseau WAN (comme décrit au § 7.2.2.2) acquiert une adresse IP de réseau WAN-Data pour une interface WAN-Data qui va utiliser une adresse IP distincte de celle de l'interface WAN-Man, le client CDC DOIT inclure l'option d'identificateur de client (objet cabhCdpWanDataAddrClientId) dans le message DHCP DISCOVER. Pour activer ces identificateurs uniques de client de réseau WAN-Data, le client CDC DOIT permettre au système NMS de créer des entrées d'objet cabhCdpWanDataAddrClientId dans la table cabhCdpWanDataAddrTable.

Si un service portail fonctionne en mode 2 d'adresse de réseau WAN (comme décrit au § 7.2.2.2) le client CDC DOIT essayer d'obtenir une adresse IP, par protocole DHCP, pour chaque identificateur de client unique (objet cabhCdpWanDataAddrClientId) dans la table cabhCdpWanDataAddrTable, jusqu'à la limite définie par l'objet cabhCdpWanDataIpAddrCount.

Le client CDC DOIT continuer à retransmettre le message DHCP DISCOVER en mettant en œuvre un algorithme exponentiel d'attente aléatoire de données compatible avec celui qui est décrit dans le document RFC 2131. Le client CDC DOIT transmettre jusqu'à 5 messages DHCP DISCOVER (un message initial plus 4 tentatives de retransmission) avant de réinitialiser à zéro la valeur du temporisateur d'attente de données et de répéter le processus.

Si le client CDC réussit à acquérir une adresse IP de réseau WAN-Man (c'est-à-dire s'il reçoit un message DHCP ACK du serveur DHCP via l'interface de réseau WAN-Man du service PS) dès la première tentative, ET si le service PS fonctionne en mode d'approvisionnement DHCP, le service PS DOIT tenter une synchronisation de la date et de l'heure avec le serveur ToD en envoyant une requête ToD comme décrit au § 7.4.3 avant de tenter de télécharger le fichier de configuration du service PS.

Si le client CDC ne réussit pas à acquérir l'adresse IP de réseau WAN-Man (c'est-à-dire si la requête DHCP arrive à expiration conformément au document RFC 2131) lors de sa première tentative, le service PS DOIT déclencher le serveur CDS (c'est-à-dire lancer le fonctionnement du serveur CDS) de façon que ce dernier puisse répondre aux requêtes DHCP provenant de dispositifs IP de réseau LAN situés dans le secteur LAN-trans.

Le client CDC ne DOIT répondre aux messages DHCP – ou en envoyer – que par l'intermédiaire d'une interface avec un réseau WAN.

Lorsque la location DHCP de réseau WAN-MAN arrive à expiration, le client CDC DOIT libérer toutes les entrées extraites des rangées de la table cabhCdpWanDnsServerTable.

En attendant que la base MIB d'objets cabhPsDevProvState ait la valeur 'pass(1)' indiquant que le processus d'approvisionnement est complet, le service PS DOIT, à l'interface avec le réseau WAN, bloquer le trafic entrant qui ne constitue pas une réponse à une requête de réseau LAN-à-WAN reçue de l'élément de services PS proprement dit ou d'un dispositif IP de réseau LAN. Ce blocage contribuera à la protection contre d'éventuelles attaques de piratage pendant le processus d'approvisionnement et pendant l'inactivation du pare-feu du service PS.

7.3 Architecture de configuration globale des services PS

7.3.1 Directives pour la conception du système de configuration globale des services PS

Les directives de conception de système suivantes retracent les fonctionnalités définies pour l'utilitaire de configuration globale des services PS.

Tableau 7-10/J.191 – Directives pour la conception d'un système global de services portail

Numéro	Directives pour la conception du système de configuration globale des services PS (BPSC)
BPSC 1	Il est nécessaire de fournir un mécanisme permettant au service PS de télécharger et de traiter les fichiers de configuration.

7.3.2 Description du système de configuration globale des services PS

La configuration globale des services PS est typiquement effectuée pendant l'approvisionnement de l'élément de services PS, via le traitement des réglages de configuration contenus au sein d'un fichier de configuration. Cependant, ce processus peut être initialisé à tout moment. L'utilitaire de configuration globale des services PS comporte les composants suivants:

1) le format du fichier de configuration;
2) les modes de déclenchement du processus de téléchargement;
3) les moyens d'authentification du fichier;
4) les moyens de signaler l'état de téléchargement du fichier de configuration PS et d'autres considérations.

La configuration globale des services PS (BPSC, *bulk PS configuration*) est un utilitaire que les opérateurs peuvent utiliser pour changer en bloc les réglages de configuration du service portail, via un fichier de configuration. En principe, le fichier de configuration PS va contenir de nombreux réglages, dans la mesure où la principale utilité des fichiers de configuration est leur capacité à changer un certain nombre de réglages de configuration avec le minimum d'intervention de la part du câblo-opérateur.

Le processus de configuration globale des services PS peut se comporter de la même façon que des réglages SNMP successifs exécutés manuellement par un opérateur. Le fichier de configuration PS

est un utilitaire destiné à rendre les opérateurs plus productifs et moins enclins à commettre des erreurs lors des grands changements de configuration.

Il est significatif de noter qu'un service portail fonctionnant en mode d'approvisionnement SNMP n'a pas besoin d'avoir un fichier de configuration PS chargé avant de commencer à fonctionner. On suppose qu'un service portail fonctionnant en mode d'approvisionnement SNMP s'initialisera lui-même dans un état connu et qu'un service portail puisse fonctionner pendant toute sa durée de vie sans charger de fichier de configuration. Cependant, un service portail acceptera et traitera un fichier de configuration PS lorsqu'on lui en fournira un.

Le téléchargement du fichier de configuration du pare-feu utilise une procédure analogue à celle du téléchargement de paramètres de configuration globale des services PS. Voir le § 11.3.5.2 pour une description de la procédure de téléchargement du fichier de configuration du pare-feu.

7.3.3 Exigences relatives à la configuration globale des services PS

Un dispositif PS fonctionnant en mode d'approvisionnement DHCP DOIT télécharger et traiter un fichier de configuration PS.

Un dispositif PS fonctionnant en mode d'approvisionnement SNMP DOIT être capable de fonctionner sans fichier de configuration PS, mais DOIT être capable de télécharger et de traiter un fichier de configuration PS s'il est déclenché comme décrit dans le § 7.3.3.2.

Les réglages d'objet de base MIB transmis dans le ficher de configuration PS ont priorité sur les réglages d'objet de base MIB existants et DOIVENT les remplacer par surécriture.

7.3.3.1 Exigences de format du fichier de configuration

Les données de configuration du service portail DOIVENT être contenues dans un fichier, qui est téléchargé par protocole TFTP. Le fichier de configuration PS DOIT contenir un certain nombre de réglages de configuration (1 par paramètre), chacun étant de la forme "Type-Longueur-Valeur (TLV)". Les définitions de ces termes sont fournies par le Tableau 7-11.

Tableau 7-11/J.191 – Définitions des nuplets TLV

Type	Identificateur d'un seul octet qui définit le paramètre
Longueur	Un ou plusieurs octets spécifiant la longueur du champ Valeur (non inclus les champs de type et de longueur)
Valeur	Ensemble d'octets de longueur définie par le terme 'longueur', contenant la valeur spécifique pour le paramètre

Les réglages de configuration DOIVENT se suivre l'un l'autre directement dans le fichier, qui est un flux d'octets (sans marqueurs d'enregistrement). Le service PS DOIT être capable de recevoir et de traiter correctement un fichier de configuration PS complété (par bourrage) à un multiple de 32 bits, ET être capable de recevoir et de traiter correctement un fichier de configuration non complété à un multiple de 32 bits. Voir au § 7.3.3.1.1 la définition du bourrage. Les réglages de configuration se divisent en trois types:

- réglages de configuration normalisés, qui doivent obligatoirement être présents;
- réglages supplémentaires ou facultatifs de configuration qui PEUVENT être présents;
- réglages de configuration spécifiques du vendeur.

Le fichier de configuration PS PEUT contenir de nombreux paramètres différents, mais les seuls paramètres qui DOIVENT être inclus dans tout fichier de configuration PS sont le marqueur de fin de données (type 255) et la vérification MIC (type 53) du service PS.

Afin de permettre une gestion uniforme des dispositifs conformes à la présente Recommandation, ceux-ci DOIVENT accepter un fichier de configuration PS ayant une longueur pouvant atteindre 64K octets.

Chaque élément de services PS DOIT accepter les types de paramètres de configuration 0, 9, 10, 21, 28, 32, 33, 34, 38, 43, 53 et 255, qui sont décrits dans le présent paragraphe et qu'un fichier de configuration PS PEUT inclure.

La longueur de la valeur contenue dans le champ de longueur concernant tout paramètre de configuration inclus dans un fichier de configuration PS DOIT être de 2 octets.

La valeur du champ Longueur pour chaque type décrit aux § 7.3.3.1.1, 7.3.3.1.2, 7.3.3.1.3, 7.3.3.1.4, 7.3.3.1.5, 7.3.3.1.6, 7.3.3.1.7 et 7.3.3.1.8 est la longueur réelle en octets du champ Valeur.

7.3.3.1.1 Réglage de configuration du bourrage

Ce réglage n'a pas de champ Longueur ou Valeur et n'est utilisé qu'à la fin du marqueur de données pour compléter le fichier à un nombre entier de mots de 32 bits.

Type	Longueur	Valeur
0	–	–

7.3.3.1.2 Nom de fichier de mise à jour logicielle

Nom du fichier de mise à jour logicielle pour le dispositif IPCable2Home. Ce nom de fichier est un nom pleinement qualifié de chemin de répertoire. Le fichier est supposé résider dans un serveur TFTP identifié dans une option de réglage de configuration.

Type	Longueur	Valeur
9	Variable	Nom de fichier

7.3.3.1.3 Commande SNMP d'accès en écriture

Cet objet rend possible de désactiver l'accès SNMP "de mise à jour" d'objets de base MIB individuels. Chaque instance de cet objet commande l'accès à tous les objets de base MIB inscriptibles dont les préfixes d'identificateur d'objet (OID, *object identifier*) correspondent. Cet objet peut être répété afin de désactiver l'accès à un nombre quelconque d'objets de base MIB.

Type	Longueur	Valeur
10	n	Préfixe d'identificateur OID plus fanion de commande

La valeur n est la taille du codage ASN.1 en règles de codage de base [Rec. UIT-T X.690 | ISO/CEI 8825-1] du préfixe de l'identificateur d'objet plus un octet pour le fanion de commande.

Le fanion de commande peut prendre les valeurs suivantes:

– 0 – accès autorisé;

– 1 – accès interdit.

Tout préfixe d'identificateur OID peut être utilisé. L'identificateur OID vide 0.0 peut être utilisé pour commander l'accès à tous les objets de base MIB. (L'identificateur OID 1.3.6.1 aura le même effet.)

Lorsque des instances multiples de cet objet sont présentes et se recouvrent, le plus long préfixe (le plus spécifique) a priorité.

L'on peut donc avoir par exemple:

– la table someTable est d'accès interdit en écriture;

– la table someTable.1.3 est d'accès autorisé en écriture.

Cet exemple interdit l'accès à tous les objets contenus dans la table someTable sauf ceux de la table someTable.1.3.

7.3.3.1.4 Serveur TFTP de mise à jour logicielle

Adresse IP du serveur TFTP dans lequel réside le fichier de mise à jour logicielle pour le dispositif IPCable2Home.

Type	Longueur	Valeur
21	4	ip1, ip2, ip3, ip4

7.3.3.1.5 Objet de base MIB du protocole SNMP avec extension de longueur

Cet objet permet d'établir des objets arbitraires de base MIB en protocole SNMP via le processus TFTP d'enregistrement, où la valeur est une liaison variable (VarBind) du protocole SNMP, comme défini dans RFC 1157. La valeur VarBind est codée en ASN.1 conformément aux règles de codage de base, exactement comme si elle faisait partie d'une demande de mise à jour SNMP.

Type	Longueur	Valeur
28	Variable	Liaison variable

Le service portail DOIT traiter la liaison variable, contenue dans un nuplet TLV de type 28, comme si elle faisait partie d'une demande de mise à jour SNMP, avec les précautions suivantes:

- le service PS DOIT traiter la demande comme étant pleinement autorisée (il ne peut pas refuser la demande en raison d'une absence de privilège);
- les dispositions de commande d'écriture SNMP (voir le paragraphe précédent) ne s'appliquent pas;
- aucune réponse SNMP n'est générée par le service portail;
- cet objet PEUT être répété avec différentes valeurs VarBind afin de mettre à jour ("Set") un certain nombre d'objets de base MIB. Toutes les mises à jour SNMP contenues dans un fichier de configuration PS DOIVENT être traitées comme si elles étaient simultanées. Chaque valeur VarBind DOIT être limitée à 65 535 octets.

7.3.3.1.6 Certificat de vérification de code de constructeur

Certificat de vérification de code de constructeur (M-CVC, *manufacturer's code verification certificate*) pour le téléchargement de logiciel sécurisé (voir § 11.3.7.5.2).

Type	Longueur	Valeur
32	Variable	Certificat CVC du constructeur (Notation ASN.1 codée en règles DER)

7.3.3.1.7 Certificat de vérification de code de cosignataire

Certificat de vérification de code de cosignataire (C-CVC, *co-signer's code verification certificate*) pour la sécurisation du téléchargement de logiciel (voir § 11.3.7.5.2).

Type	Longueur	Valeur
33	Variable	Certificat CVC de cosignataire (Notation ASN.1 codée en règles DER)

7.3.3.1.8 Valeur de démarrage SNMPv3

(Voir § B.C.1.2.8 de l'Annexe B à la Rec. UIT-T J.112.)

Les éléments de services portail conformes DOIVENT comprendre le nuplet TLV suivant et ses sous-éléments et être capables d'ouvrir l'accès SNMPv3 au service portail, que celui-ci fonctionne en mode NmAccess ou en mode de coexistence (voir les § 6.3.3 et 6.3.6).

Type	Longueur	Valeur
34	n	Composite

Jusqu'à cinq de ces objets peuvent être inclus dans le fichier de configuration. Chacun de ces objets se traduit par l'adjonction d'une rangée additionnelle aux tables usmDHKickstartTable et usmUserTable et par la génération d'un numéro public d'agent pour ces rangées.

7.3.3.1.8.1 Nom de sécurité de démarrage SNMPv3

Type	Longueur	Valeur
34.1	2-16	Nom de sécurité codé en caractères UTF8

Pour le jeu de caractères ASCII, les codages UTF8 et ASCII sont identiques. Normalement, ce codage est spécifié comme étant un des utilisateurs du modèle USM intégré dans le système DOCSIS, par exemple: "docsisManager", "docsisOperator", "docsisMonitor", "docsisUser".

Le nom de sécurité N'EST PAS terminé par zéro, ce qui est signalé dans la table usmDHKickStartTable comme étant un nom de l'objet usmDHKickStartSecurityName et dans la table usmUserTable comme étant un nom des objets usmUserName et usmUserSecurityName.

7.3.3.1.8.2 Numéro public de gestionnaire de démarrage SNMPv3

Type	Longueur	Valeur
34.2	n	Numéro public à codage de Diffie-Helman du gestionnaire, exprimé comme une chaîne d'octets

Ce nombre est le numéro public à codage de Diffie-Helman déduit d'un nombre aléatoire généré de façon privée (par le gestionnaire ou par l'opérateur) et transformé conformément au document RFC 2786. Ce nombre est rapporté dans la table usmDHKickStartTable comme faisant partie de l'objet usmKickstartMgrPublic. Lorsqu'il est combiné avec l'objet rapporté dans la même rangée comme faisant partie de l'objet usmKickstartMyPublic, ce nombre peut servir à calculer les clés dans la rangée correspondante de la table usmUserTable.

7.3.3.1.9 Elément de fichier de configuration PS – Récepteur de notification docsisv3

Type	Longueur	Valeur
38	N	Composite

Cet élément de fichier de configuration PS spécifie une station de gestion de réseau qui va recevoir des notifications de la part du service portail lorsque celui-ci est en mode de gestion de réseau "coexistence". Ce nuplet TLV (38) se compose de plusieurs sous-champs TLV contenus dans l'élément de fichier de configuration PS par nuplets TLV. Jusqu'à dix de ces éléments peuvent être inclus dans le fichier de configuration PS. Le § 6.3.6.4 donne des détails sur la façon dont cet élément du fichier de configuration PS est mappé dans les tables fonctionnelles SNMPv3.

NOTE – Tous les champs à octets multiples d'un sous-nuplet TLV doivent être placés dans l'ordre des octets du réseau.

7.3.3.1.9.1 Sous-TLV 38.1 – Adresse IP du récepteur de transfert

Adresse IP du récepteur de transfert, en binaire.

Type	Longueur	Valeur
38.1	4	Adresse IP

7.3.3.1.9.2 Sous-TLV 38.2 – Numéro de point d'accès UDP du récepteur de transfert

Numéro de point d'accès UDP du récepteur de transfert, en binaire.

Type	Longueur	Valeur
38.2	2	Accès UDP

(Si ce champ est absent, on utilise la valeur par défaut 162.)

7.3.3.1.9.3 Sous-TLV 38.3 – Type de transfert envoyé par le service PS

Type de transfert

Type	Longueur	Valeur
38.3	2	Type de transfert

Les valeurs suivantes de type de transfert DOIVENT être reconnues:

– 1 = message TRAP du protocole SNMP v1 dans un paquet SNMP v1;
– 2 = message TRAP du protocole SNMP v2c dans un paquet SNMP v2c;
– 3 = message INFORM du protocole SNMP dans un paquet SNMP v2c;
– 4 = message TRAP du protocole SNMP v2c dans un paquet SNMP v3;
– 5 = message INFORM du protocole SNMP dans un paquet SNMP v3;

7.3.3.1.9.4 Sous-TLV 38.4 – Temporisation

Temporisation, en millisecondes, utilisée pour envoyer les messages INFORM du protocole SNMP.

Type	Longueur	Valeur
38.4	2	0-65535

7.3.3.1.9.5 Sous-TLV 38.5 – Nombre d'essais d'envoi d'un message INFORM, après l'avoir envoyé une première fois

Type	Longueur	Valeur
38.5	2	0-65535

7.3.3.1.9.6 Sous-TLV 38.6 – Paramètres de filtrage de notification

Type	Longueur	Valeur
38.6	n	OID de filtre

où n est la longueur de l'identificateur d'objet à codage ASN.1.

Si ce sous-TLV est absent, le récepteur de notification recevra toutes les notifications générées par l'agent SNMP.

Il s'agit d'un identificateur d'objet (OID) de filtre formaté en ASN.1, de valeur snmpTrapOID qui identifie les notifications à envoyer au récepteur de notification. Cette notification sera envoyée avec tout ce qu'elle recouvre.

7.3.3.1.9.7 Sous-TLV 38.7 – Nom de sécurité à utiliser lors de l'envoi d'une notification SNMP v3

Type	Longueur	Valeur
38.7	2-16	Nom de sécurité codé en format UTF8

Ce sous-TLV n'est pas exigé pour les messages TRAP de type = 1, 2, ou 3 ci-dessus (s'il est présent, il doit être ignoré). S'il n'est pas approvisionné avec un type 4 ou 5 de transfert, la notification v3 sera alors envoyée avec le niveau de sécurité noAuthNoPriv au moyen du nom de sécurité "@PSconfig" (Note 2).

Nom de sécurité:

nom de sécurité v3 à utiliser lors de l'envoi d'une notification v3. Il n'est utilisé que si le type de transfert est réglé à 4 ou 5. Ce DOIT être un nom spécifié dans un nuplet TLV de type 34 de fichier de configuration PS en tant que partie de la procédure de démarrage DH (Diffie-Helman). Les notifications seront envoyées au moyen des clés d'authentification et de confidentialité calculées par le service portail pendant la procédure de démarrage DH (Diffie-Helman).

NOTE 1 – Dès réception de l'un de ces éléments de TLV, le service portail DOIT constituer des entrées dans les tables suivantes afin de provoquer la transmission de transfert désirée: snmpNotifyTable, snmpTargetAddrTable, snmpTargetParamsTable, snmpNotifyFilterProfileTable, snmpNotifyFilterTable, snmpCommunityTable, usmUserTable, vacmSecurityToGroupTable, vacmAccessTable et vacmViewTreeFamilyTable.

NOTE 2 – Type de transfert: la chaîne de communauté pour les transfert dans les paquets SNMP v1 et v2 DOIT être "public". Le nom de sécurité dans les messages TRAP et INFORM des paquets SNMP v3 où il n'a pas été spécifié de nom de sécurité DOIT être "@PSconfig" et, dans ce cas, le niveau de sécurité DOIT être à la valeur noAuthNoPriv.

NOTE 3 – OID de filtre: la version SNMP v3 permet la spécification des identificateurs OID de transfert qui sont à envoyer à un récepteur de transfert. L'identificateur OID de filtre situé dans l'élément de fichier de configuration PS spécifie l'identificateur OID de la racine d'un sous-arbre de filtre de transfert. Tous les messages TRAP avec un OID de transfert contenu dans ce sous-arbre de filtre de transfert DOIVENT être envoyés au récepteur de transfert.

NOTE 4 – Le fichier de configuration PS PEUT aussi contenir des éléments MIB de nuplet TLV qui constituent des entrées dans n'importe laquelle des 10 tables dont la liste figure dans la Note 1. Ces éléments MIB de nuplet TLV NE DOIVENT PAS utiliser les colonnes d'index qui commencent par les caractères "@PSconfig".

NOTE 5 – Cet élément de nuplet TLV ne DOIT être traité que si le service portail est passé en mode de coexistence SNMP v3 pendant le traitement du fichier de configuration PS.

7.3.3.1.10 Informations spécifiques du vendeur

Les informations spécifiques du vendeur pour le service PS, si elles sont présentes, DOIVENT être codées dans le champ d'informations spécifiques du vendeur (VSIF, *vendor specific information field*) (code 43) au moyen du champ d'identificateur de vendeur afin de spécifier quels nuplets TLV s'appliquent à quels produits de vendeurs. L'identificateur de vendeur DOIT être le premier sous-TLV imbriqué dans le champ VSIF. Si le premier nuplet TLV contenu dans le champ VSIF n'est pas un identificateur de vendeur, le fichier de configuration PS DOIT être ignoré.

Ce réglage de configuration peut apparaître plusieurs fois. Le même identificateur de vendeur peut apparaître plusieurs fois. Il ne DOIT PAS y avoir plus d'un seul sous-TLV d'identificateur de vendeur dans un même champ VSIF.

Type	Longueur	Valeur
43	n	Réglages spécifiques du vendeur

7.3.3.1.10.1 Sous-TLV 43.1 – Type d'identificateur de vendeur

Identification de vendeur spécifiée par les 3 octets de l'identificateur unique d'organisation (OUI, *organization unique identifier*) du vendeur PS.

Type	Longueur	Valeur
43.1	3	v1, v2, v3

7.3.3.1.11 Marqueur de fin de données

C'est un marqueur spécial pour la fin des données. Il ne comporte pas de champs de longueur ou de valeur.

Type	Longueur	Valeur
255	–	–

7.3.3.1.12 Vérification d'intégrité de message PS (MIC de PS)

Type	Longueur	Valeur
53	20	Hachage SHA sur 160 bits (20 octets)

Ce paramètre contient un hachage (vérification MIC de PS) calculé par un algorithme de hachage sécurisé (SHA-1) défini dans le document FIPS 180-2. Ce nuplet TLV n'est utilisé que dans le fichier de configuration PS, immédiatement avant la fin du marqueur de données.

7.3.3.2 Mode de déclenchement

Le transfert du fichier de configuration, entre le serveur TFTP situé dans le système de tête de réseau et l'élément de services PS, est initialisé par un événement désigné par le terme de *déclencheur*. Les exigences relatives au déclenchement du transfert d'un fichier de configuration PS du serveur TFTP au service portail sont données ci-après.

Le mode de déclenchement du téléchargement du fichier de configuration PS dépend du mode d'approvisionnement dans lequel fonctionne le service portail. Le portail CMP DOIT lire la valeur de l'objet cabhPsDevProvMode (voir § 7.2.3.3) avant d'initialiser un téléchargement de fichier de configuration PS.

Déclenchement du téléchargement de fichier de configuration PS dans le mode d'approvisionnement DHCP:

si le service portail reçoit l'adresse du serveur TFTP dans le champ "siaddr" et le nom de fichier de configuration PS dans le champ "file" du message DHCP ACK, le service portail DOIT combiner l'adresse du serveur TFTP et le nom de fichier de configuration PS pour former une valeur codée sous forme de localisation URL et écrire cette valeur dans l'objet cabhPsDevProvConfigFile. Le service PS DOIT utiliser le format suivant pour la valeur codée sous forme de localisation URL de l'adresse du serveur TFTP et du nom de fichier de configuration PS:

tftp://adresse IPv4 du serveur TFTP/chemin complet du fichier de configuration PS/nom du fichier de configuration PS

Le téléchargement du fichier de configuration PS par un service portail fonctionnant en mode d'approvisionnement DHCP est déclenché par la présence de la localisation du fichier de configuration PS (adresse IP de serveur TFTP) et de son nom dans le message DHCP présenté au service portail (client CDC) par le serveur DHCP dans le réseau câblé. Voir le § 7.2.3.3.

Si le service portail fonctionne en mode d'approvisionnement DHCP (comme indiqué par la valeur de l'objet cabhPsDevProvMode), après réception par le service portail (client CDC) d'un message DHCP ACK provenant du serveur DHCP dans le réseau câblé, le service portail DOIT envoyer une requête TFTP Get adressée au serveur identifié dans le champ "siaddr" du message DHCP, afin de télécharger le fichier identifié dans le champ "file" du message DHCP.

Le dispositif PS NE DOIT envoyer de messages de demande Get du protocole TFTP que par l'intermédiaire de l'interface PS WAN-Man.

La modification de l'objet cabhPsDevProvConfigFile NE DOIT PAS déclencher le téléchargement, par un dispositif PS fonctionnant en mode d'approvisionnement DHCP, d'un fichier de configuration. Un dispositif PS fonctionnant en mode d'approvisionnement DHCP DOIT traiter l'objet cabhPsDevProvConfigFile comme étant en lecture seule.

Le dispositif PS DOIT rejeter tout fichier de configuration PS qui est reçu par l'intermédiaire de toute autre interface que l'interface PS WAN-Man.

Déclenchement du téléchargement de fichier de configuration PS dans le mode d'approvisionnement SNMP:

si le service portail fonctionne en mode d'approvisionnement SNMP (comme indiqué par la valeur de l'objet cabhPsDevProvMode), le téléchargement du fichier de configuration PS NE DOIT PAS survenir avant l'achèvement du processus d'authentification SNMP v3 (voir au § 11 des précisions sur le processus d'authentification SNMP).

Si le service portail fonctionne en mode d'approvisionnement SNMP (comme indiqué par la valeur de l'objet cabhPsDevProvMode), l'élément de services PS NE DOIT PAS initialiser un téléchargement de fichier de configuration PS si une valeur valide pour cabhPsDevProvConfigHash (base MIB PSDev) n'a pas été approvisionnée par le système NMS.

Une fois que le service portail fonctionnant en mode d'approvisionnement SNMP (comme indiqué par la valeur de l'objet cabhPsDevProvMode) émet une requête TFTP afin de télécharger un fichier de configuration PS (sous réserve des conditions décrites ci-dessous dans d'autres exigences), le service PS DOIT achever la phase de téléchargement. Lorsque le service PS (portail CMP) a correctement téléchargé le fichier de configuration PS demandé, il DOIT traiter ce fichier avant d'émettre une requête TFTP concernant un autre fichier de configuration PS.

Un mécanisme de signalisation est nécessaire afin d'informer l'entité de gestion du fait que le service PS est actuellement en train de traiter un fichier de configuration PS. L'objet cabhPsDevProvConfigFileStatus de la base MIB Dev du service PS est défini de façon à constituer ce mécanisme de signalisation.

Si un service PS (portail CMP) n'est pas déjà en train de demander, de télécharger ou de traiter un fichier de configuration PS, ce service DOIT mettre l'objet cabhPsDevProvConfigFileStatus = idle(1). Lorsque le service PS (portail CMP) a émis une demande de fichier de configuration PS spécifié dans l'objet cabhPsDevProvConfigFile, il doit mettre l'objet cabhPsDevProvConfigFileStatus = busy(2). Lorsque le service PS

(portail CMP) a terminé le traitement du fichier de configuration PS, le service PS doit mettre l'objet cabhPsDevProvConfigFileStatus = idle(1).

Lorsqu'il reçoit un message de demande d'établissement SNMP pour l'objet cabhPsDevProvConfigFile, le service PS (portail CMP) DOIT essayer de télécharger et de traiter le fichier de configuration PS dont le nom et l'adresse sont spécifiés dans l'objet cabhPsDevProvConfigFile, si les conditions suivantes sont vérifiées:

- le service PS fonctionne en mode d'approvisionnement SNMP;
- l'objet cabhPsDevProvConfigHash a une valeur valide; ET
- l'objet cabhPsDevProvConfigFileStatus = idle(1).

Le format de l'objet cabhPsDevProvConfigFile DOIT être une adresse IP de serveur TFTP codée sous forme de localisation URL et un nom de fichier de configuration.

Si le service PS (portail CMP) fonctionnant en mode d'approvisionnement SNMP reçoit une demande SNMP de mise à jour issue du système NMS afin de mettre à jour la valeur des objets cabhPsDevProvConfigFile ET cabhPsDevProvConfigFileStatus à la valeur = busy(2) OU si l'objet cabhPsDevProvConfigHash ne possède pas de valeur valide, alors le service PS DOIT rejeter cette demande de mise à jour.

Fonctionnement après déclenchement:

Une fois déclenché, le service portail DOIT utiliser un client TFTP conforme au document RFC 1350 afin de télécharger les fichiers de configuration du service PS.

Une fois déclenché afin de télécharger un fichier de configuration PS, l'élément de services PS DOIT continuer à essayer de télécharger le fichier de configuration PS spécifié à partir de l'emplacement spécifié, jusqu'à ce que ce fichier de configuration PS ait été correctement téléchargé et que le hachage ait été correctement calculé comme décrit au § 7.3.3.3. Si la première tentative échoue, le service PS DOIT utiliser une temporisation adaptative pour le protocole TFTP sur la base d'un temps exponentiel d'attente de données binaires comme décrit ci-dessous, jusqu'à ce que le service PS (portail CMP) reçoive correctement le fichier recherché du serveur TFTP situé à la tête du réseau:

- chaque réessai a lieu 2^n seconde(s) après la tentative précédente, où le compteur de réessais du fichier de configuration PS, n = [0, 1, 2, 3, 4 ou 5];
- n = 0 pour le premier réessai, puis est incrémenté d'une unité à chaque nouvelle tentative jusqu'à ce que n = 5;
- si le service PS n'obtient pas correctement le fichier demandé après la tentative où n = 5, n est remis à zéro et le service PS doit relancer le processus d'acquisition IP de réseau WAN-Man par le protocole DHCP.

Le service PS ne DOIT échanger de messages TFTP que par l'interface avec le réseau WAN-Man du service PS. Celui-ci DOIT rejeter tout fichier de configuration PS non reçu par l'intermédiaire de l'interface avec le réseau WAN-Man du service PS.

Lorsque le téléchargement par protocole TFTP du fichier de configuration PS est terminé ET que ce fichier est correctement authentifié comme décrit au § 7.3.3.3, le service PS DOIT traiter comme défini ci-dessous les nuplets TLV contenus dans ce fichier. L'on trouvera au § 7.3.3.4 des détails concernant le traitement des erreurs et la génération d'événement au cours du traitement du fichier de configuration PS.

Le service PS DOIT utiliser les paramètres extraits du fichier de configuration PS afin de régler la valeur des objets gérés dans la base de données du service PS. Ce processus équivaut, en termes de fonction, à une opération de mise à jour SET du protocole SNMP mais il ne dépend pas de l'utilisateur ou des autorisations d'accès fondées sur le point de vue. Le service PS DOIT inconditionnellement mettre à jour les objets gérés correspondant à des identificateurs OID reconnus dans la base de données du service PS.

Le service PS DOIT convertir les éléments TLV-28 du fichier de configuration PS en une unique unité PDU du protocole SNMP contenant (n) composants d'identificateur OID ou d'instance et valeur (éléments 'varbinds' du protocole SNMP). Conformément au document RFC 1905, l'unique unité PDU SNMP générée par un fichier de configuration PS sera traitée "comme si elle était simultanée" et le service PS doit avoir un comportement cohérent, quel que soit l'ordre dans lequel les éléments TLV-28 apparaissent dans le fichier de configuration PS ou dans l'unité PDU du protocole SNMP. La règle concernant l'unique unité PDU du protocole SNMP générée par un fichier de configuration PS est compatible avec les comportements des paquets SNMP d'unité PDU reçus d'un gestionnaire SNMP; l'ordre des valeurs 'varbind' des unités PDU du protocole SNMP n'a pas d'importance et aucune limite MAX n'est fixée à ces unités. Une fois qu'une unique unité PDU est construite en protocole SNMP, le service PS la traite et détermine l'acceptation/le rejet de la configuration du service PS sur la base des règles de traitement du fichier de configuration PS décrites au § 7.3.3.4.

La longueur du fichier de configuration PS DOIT être mise à jour dans l'objet cabhPsDevProvConfigFileSize de base MIB.

Le nombre de nuplets TLV traités (c'est-à-dire destinés à changer la configuration du service PS conformément à leur propre champ de valeur) et le nombre de nuplets TLV ignorés (c'est-à-dire destinés à changer la configuration du service PS conformément à leur propre champ de valeur mais qui n'y réussissent pas) DOIVENT être mis à jour dans les objets de base MIB cabhPsDevProvConfigTLVProcessed et cabhPsDevProvConfigTLVRejected respectivement. Les types de paramètres de configuration 255 (Marqueur de fin de données), 53 (Vérification MIC du service PS), 0 (Réglage de configuration du bourrage) et les paires de type-longueur qui correspondent à des sous-TLV ne spécifient aucune valeur dans les champs de valeur destinés à modifier la configuration du service PS et donc NE DOIVENT PAS être comptés dans les valeurs des objets cabhPsDevProvConfigTLVProcessed et cabhPsDevProvConfigTLVRejected.

Conformément à ces définitions, un nuplet TLV qui ne réussit pas à configurer le service PS est compté deux fois, c'est-à-dire une fois par chacun des objets cabhPsDevProvConfigTLVProcessed et cabhPsDevProvConfigTLVRejected. Un nuplet TLV qui réussit à configurer le service PS n'est compté que par l'objet cabhPsDevProvConfigTLVProcessed.

7.3.3.3 Moyens d'authentification du fichier de configuration PS

Le présent paragraphe définit la procédure d'authentification du fichier de configuration PS.

L'algorithme utilisé pour authentifier le hachage du fichier de configuration PS dépend du mode d'approvisionnement de l'élément de services PS (voir § 5.5). Il y a deux types de modes d'approvisionnement: le mode d'approvisionnement DHCP et le mode d'approvisionnement SNMP. Les paragraphes suivants décrivent les algorithmes de sécurité et les exigences nécessaires pour vérifier le hachage du fichier de configuration PS sur la base du mode d'approvisionnement de l'élément de services PS, lequel DOIT accepter les deux algorithmes de sécurité spécifiés aux § 7.3.3.3.1 et 7.3.3.3.2.

7.3.3.3.1 Algorithme d'authentification de fichier de configuration PS pour le mode d'approvisionnement DHCP

La procédure de vérification du hachage du fichier de configuration PS par l'élément de services PS en mode d'approvisionnement DHCP est la suivante:

1) lorsque le générateur de fichier de configuration PS du système NMS crée un nouveau fichier de configuration PS ou modifie un fichier existant, le générateur de fichier de configuration PS du système NMS va créer un hachage SHA-1 du contenu du fichier de

configuration PS considéré comme une chaîne d'octets. Le marqueur de fin de données et tout bourrage lui faisant suite ne sont pas inclus dans le calcul de hachage;

2) le générateur de fichier de configuration PS du système NMS ajoute au fichier de configuration PS la valeur de hachage calculée à l'étape 1 en tant que dernier réglage par nuplet TLV (immédiatement avant le marqueur de fin de données) au moyen d'un nuplet TLV de type 53. Le fichier de configuration PS est ensuite mis à la disposition du serveur TFTP approprié;

3) l'élément de services PS télécharge le fichier de configuration PS;

4) le service PS DOIT mettre à jour l'objet cabhPsDevProvConfigHash de base MIB au moyen de la valeur de hachage extraite du nuplet TLV de hachage créé aux étapes 1 et 2;

5) l'élément de services PS DOIT calculer un hachage SHA-1 sur le contenu du fichier de configuration PS à l'exception du nuplet TLV de hachage (utilisé pour configurer l'objet cabhPsDevProvConfigHash de base MIB), à l'exception du marqueur de fin de données et à l'exception de tout bourrage subséquent. Si le hachage calculé et la valeur de l'objet cabhPsDevProvConfigHash de base MIB sont identiques, l'intégrité du fichier de configuration PS est vérifiée et le fichier de configuration PS DOIT être traité; sinon, il DOIT être rejeté.

7.3.3.3.2 Algorithme d'authentification de fichier de configuration PS pour le mode d'approvisionnement SNMP

La procédure de vérification du hachage du fichier de configuration PS par l'élément de services PS en mode d'approvisionnement SNMP est la suivante:

1) lorsque le générateur de fichier de configuration PS du système NMS crée un nouveau fichier de configuration PS ou modifie un fichier existant, le générateur de fichier de configuration PS va créer un hachage SHA-1 du contenu entier du fichier de configuration PS considéré comme une chaîne d'octets. Le marqueur de fin de données et tout bourrage lui faisant suite ne sont pas inclus dans le calcul de hachage;

2) le système NMS envoie la valeur de hachage calculée à l'étape 1 à l'élément de services PS au moyen de la commande SET du protocole SNMP. Le service PS met à jour son objet cabhPsDevProvConfigHash de base MIB avec la nouvelle valeur;

3) le système NMS envoie le nom et l'emplacement du fichier de configuration PS au moyen de la commande SET du protocole SNMP. Le service PS met à jour son objet cabhPsDevProvConfigFile de base MIB avec la nouvelle valeur;

4) l'élément de services PS télécharge le fichier nommé à partir du serveur TFTP configuré. Si le fichier de configuration PS contient un nuplet TLV de type 53, le service PS DOIT l'ignorer;

5) l'élément de services PS DOIT calculer un hachage SHA-1 sur le contenu du fichier de configuration PS à l'exception du nuplet TLV de hachage (utilisé pour configurer l'objet cabhPsDevProvConfigHash de base MIB), à l'exception du nuplet TLV de type 53 s'il existe, à l'exception du marqueur de fin de données et à l'exception de tout bourrage subséquent. Si le hachage calculé et la valeur de l'objet cabhPsDevProvConfigHash de base MIB sont identiques, l'intégrité du fichier de configuration PS est vérifiée et le fichier de configuration PS DOIT être traité; sinon, il DOIT être rejeté.

Le téléchargement correct du fichier de configuration PS est considéré comme complet après réception correcte par l'élément de services PS du contenu du fichier de configuration PS dans la période de temporisation TFTP ET calcul par le service PS des valeurs de hachage pour le fichier de configuration PS sans erreurs de calcul.

7.3.3.4 Mode de signalisation des états

Le service portail DOIT signaler l'état et les conditions d'erreur du téléchargement du fichier de configuration PS au moyen du processus de rapport d'événement décrit au § 6.5.

Le Tableau 7-12 identifie les modes de succès et d'échec qui pourraient être rencontrés lors du téléchargement et du traitement d'un fichier de configuration PS, ainsi que l'action que le service PS DOIT entreprendre lorsqu'il détecte ces modes.

Tableau 7-12/J.191 – Mode de traitement de fichier de configuration PS

Mode d'échec	Action
Le champ Type n'est pas valide dans l'environnement IPCable2Home	Ne pas tenir compte du nuplet TLV en question et rapporter un événement. Continuer de traiter le fichier.
Le transfert TFTP a échoué – Requête GET émise mais aucune réponse reçue	Rapporter un événement (68000500) et réessayer le transfert TFTP.
Le transfert TFTP a échoué – Fichier de configuration PS non trouvé	Rapporter un événement (68000600) et réessayer le transfert TFTP.
Le transfert TFTP a échoué – Paquets dans le désordre.	Rapporter un événement (68000700) et réessayer le transfert TFTP.
Le téléchargement TFTP a échoué – Nombre maximal de réessais dépassé.	Rapporter un événement (68000900) et réinitialiser.
Le téléchargement TFTP a réussi	Rapporter un événement (68001000) et commencer à traiter le fichier.
Le fichier échoue à l'essai d'authentification	Rapporter un événement (68000800) et réinitialiser. Ne pas essayer de traiter le fichier.
Le fichier est trop gros	Rapporter un événement (73040120) et réinitialiser. Ne pas essayer de traiter le fichier.
Absence de marqueur de fin de fichier	Rapporter un événement (73040102) et réinitialiser. Ne pas essayer de traiter le fichier.
Duplication de l'identificateur OID du nuplet TLV-28	Rapporter un événement (73040102), rejeter le fichier de configuration PS et réinitialiser. Préserver toutes les valeurs d'objet qui existaient avant la tentative de traitement de ce mauvais fichier de configuration.
Type reconnu mais mauvaise valeur ou TLV-28 valide OID reconnu mais mauvaise valeur de base MIB	Rapporter un événement (73040102), rejeter le fichier de configuration PS et réinitialiser. Préserver toutes les valeurs d'objet qui existaient avant la tentative de traitement de ce mauvais fichier de configuration.
Réglage de valeur impossible	Rapporter un événement, refuser le fichier de configuration PS et réinitialiser. Rétablir toutes les valeurs (d'avant la mise à jour SNMP) qui ont été sauvegardées dans une mémoire non volatile.
Le portail CMP rencontre un identificateur OID SNMP non reconnu	Ne pas tenir compte du nuplet TLV en question et rapporter un événement (73040100). Continuer de traiter le fichier.

Voir à l'Annexe B une liste des événements y compris ceux qui sont énumérés dans le Tableau 7-12, ainsi que des informations sur la façon dont les événements sont rapportés.

Tentative infructueuse de téléchargement du fichier de configuration PS – Réessais par protocole TFTP autorisés

Si le compteur de réessais de téléchargement du fichier de configuration PS est inférieur à 5 ET si la requête GET du protocole TFTP arrive à expiration, si le fichier de configuration PS n'est pas

trouvé dans le serveur TFTP OU si la requête GET du protocole TFTP a échoué en raison d'un désordre des paquets, le service PS DOIT lancer le fonctionnement du serveur CDS et du portail CNP, rapporter l'événement approprié et réessayer de télécharger le fichier de configuration PS, conformément à l'algorithme de réessai qui est décrit au § 7.3.3.2.

Chaque fois que le service PS échoue à télécharger le fichier de configuration PS, il DOIT rapporter l'événement approprié qui est indiqué dans l'Annexe B, afin de signaler un échec de téléchargement du fichier de configuration PS.

Tentative infructueuse de téléchargement du fichier de configuration PS – Réessais par protocole TFTP épuisés

Si le compteur de réessais de téléchargement du fichier de configuration PS est égal à 5 ET si le service PS n'a pas réussi à télécharger le fichier de configuration PS, le service PS DOIT rapporter l'événement indiqué dans l'Annexe B afin de signaler un échec du processus de téléchargement du fichier de configuration PS ET libérer son adresse IP de réseau WAN-Man PS conformément au document RFC 2131 ET relancer le processus d'acquisition d'adresse IP de réseau WAN-Man par protocole DHCP.

Succès du téléchargement du fichier de configuration PS

Si le service PS réussit à télécharger le fichier de configuration PS, il DOIT remettre à zéro le compteur de réessais de téléchargement du fichier de configuration PS et rapporter l'événement approprié qui est indiqué dans l'Annexe B afin de signaler la réussite du téléchargement du fichier de configuration PS.

Si le fichier de configuration PS échoue à la vérification d'authentification spécifiée au § 7.3.3.3, le service PS DOIT arrêter le processus d'approvisionnement, rejeter le fichier de configuration PS, rapporter l'événement approprié, et relancer le processus d'acquisition d'adresse IP de réseau WAN-Man par protocole DHCP.

Si le fichier de configuration PS ne contient aucun nuplet TLV de fin EOF ou est trop gros pour être traité, le service PS DOIT arrêter le processus d'approvisionnement, rejeter le fichier de configuration PS, rapporter l'événement approprié, et relancer le processus d'acquisition d'adresse IP de réseau WAN-Man par protocole DHCP.

Si le fichier de configuration PS contient des éléments TLV-28 en double ("en double" signifiant que l'objet de base MIB du protocole SNMP possède un identificateur identique), le service PS DOIT arrêter le processus d'approvisionnement, rejeter le fichier de configuration PS, rapporter l'événement approprié, et relancer le processus d'acquisition d'adresse IP de réseau WAN-Man par protocole DHCP.

Si le fichier de configuration PS contient un champ de type reconnu mais un champ de valeur erroné ou un identificateur OID de TLV-28 valide mais une valeur de base MIB erronée, le service PS DOIT arrêter le processus d'approvisionnement, rejeter le fichier de configuration PS, rapporter l'événement approprié, et relancer le processus d'acquisition d'adresse IP de réseau WAN-Man par protocole DHCP.

Si le fichier de configuration PS contient un champ de type non reconnu ou un élément TLV-28 ayant un identificateur OID non reconnu, le service PS DOIT ignorer ce nuplet TLV, rapporter l'événement approprié ET continuer à traiter le fichier de configuration PS.

7.4 Architecture du client d'heure actuelle

7.4.1 Directives pour la conception du système de client d'heure actuelle

Les directives de conception de système suivantes décrivent les fonctionnalités définies pour le client d'heure actuelle du service portail.

Tableau 7-13/J.191 – Directives pour la conception du système de client d'heure actuelle

Numéro	Directives pour la conception du système de client d'heure actuelle
TOD 1	Il est nécessaire de fournir un mécanisme permettant au service portail de mettre en œuvre la synchronisation horaire avec la tête de réseau.

7.4.2 Description du système de client d'heure actuelle

L'élément de services PS utilise un client d'heure actuelle compatible avec le document RFC 868, afin de mettre en œuvre la synchronisation horaire avec un serveur temporel situé en tête de réseau. La synchronisation horaire est essentielle pour les fonctions de sécurité du service portail ainsi que pour les messages d'événement.

Lorsque le client DHCP du client CDC demande au serveur DHCP de tête de réseau une adresse IP pour l'interface WAN-Man, ce client DHCP va recevoir l'adresse IP du serveur temporel de tête de réseau au sein de l'option 4 DHCP. Le client DHCP recevra aussi le décalage temporel (par rapport à l'UTC), au sein de l'option 2 DHCP.

Un fois que la pile IP de réseau WAN-Man commence à utiliser l'adresse IP qu'elle a reçue du protocole DHCP, elle devrait envoyer une demande d'heure RFC 868 au serveur temporel. Si celui-ci renvoie une réponse valide, le service portail commencera à utiliser cette heure pour les marqueurs temporels des messages d'événement et pour les fonctions de sécurité.

7.4.3 Exigences relatives au client d'heure actuelle

L'élément de services PS DOIT implémenter un client d'heure actuelle.

Le client d'heure actuelle du service portail DOIT être conforme au protocole horaire du document RFC 868 et ne doit utiliser que le protocole UDP.

Lors d'un rétablissement, l'élément de services PS DOIT initialiser sa date à 00:00.0 (minuit) du 1er janvier 1970.

L'élément de services PS DOIT tenter la synchronisation horaire avec les serveurs horaires fournis par l'option 4 DHCP contenue dans le message ACK DHCP reçu par l'interface WAN-Man au cours d'une acquisition de location WAN-Man.

Si le service PS reçoit l'option 4 DHCP (option de serveur temporel) dans le message ACK DHCP, le service PS DOIT sauvegarder l'adresse IP du serveur temporel duquel le service PS a accepté une réponse, sous forme de valeur de l'objet cabhPsDevTimeServerAddr.

Le service portail DOIT combiner l'heure récupérée auprès du serveur temporel avec le décalage temporel fourni par l'option 2 du protocole DHCP afin de créer l'heure locale actuelle.

L'élément de services PS DOIT utiliser l'heure locale actuelle calculée à partir de l'heure récupérée auprès du serveur temporel et du décalage temporel reçu de l'option 2 du protocole DHCP pour toutes fonctions nécessitant l'heure actuelle, qui ne doit être exacte qu'à la seconde près.

La priorité de l'horloge d'heure actuelle du système est la suivante pour un service PS imbriqué:

- première priorité: heure acquise auprès du serveur ToD;
- deuxième priorité: heure acquise auprès du câblo-modem;
- troisième priorité: heure initialisée au 1er janvier 1970.

Un service PS imbriqué DOIT utiliser la plus récente heure valide qui a été acquise auprès du serveur ToD pour l'horloge d'heure actuelle du système, même si cela implique la surécriture du temps système acquis par le CM.

Si un service PS imbriqué n'est pas en mesure d'acquérir l'heure actuelle auprès du serveur ToD, ce service DOIT utiliser l'heure acquise par le câblo-modem pour l'horloge d'heure actuelle du système.

Si un service PS imbriqué n'est pas en mesure d'acquérir l'heure actuelle auprès du serveur ToD ET s'il n'est pas en mesure d'acquérir une heure valide auprès du câblo-modem, ce service DOIT utiliser l'heure initialisée par le processus de réamorçage au 1er janvier 1970 pour l'horloge d'heure actuelle du système.

La priorité de l'horloge d'heure actuelle du système est la suivante pour un service PS autonome:

- première priorité: heure acquise auprès du serveur ToD;
- deuxième priorité: heure initialisée au 1er janvier 1970.

Un service PS autonome DOIT utiliser la plus récente heure valide qui a été acquise auprès du serveur ToD pour l'horloge d'heure actuelle du système.

Si un service PS autonome n'est pas en mesure d'acquérir l'heure actuelle auprès du serveur ToD, ce service DOIT utiliser l'heure initialisée par le processus de réamorçage au 1er janvier 1970 pour l'horloge d'heure actuelle du système.

L'élément de services PS DOIT continuer d'essayer de communiquer avec le serveur temporel, jusqu'à l'établissement de l'heure locale. Le serveur DHCP pourrait offrir de multiples adresses IP de serveur horaire dans son message ACK DHCP. Le service PS DOIT essayer d'acquérir l'heure actuelle auprès de tous les serveurs horaires inclus dans le message ACK DHCP qu'il reçoit du serveur DHCP, jusqu'à ce que l'heure locale ait été établie. La temporisation spécifique pour les demandes d'heure dépend de l'implémentation. Cependant, pour chaque serveur identifié dans le message ACK DHCP, le client d'heure du service portail ne DOIT PAS dépasser trois demandes d'heure dans toute période de cinq minutes. Au minimum, le client d'heure du service portail DOIT produire au moins une demande d'heure par période de cinq minutes pour chaque serveur spécifié, jusqu'à ce que l'heure locale soit établie.

Si le serveur temporel ne renvoie pas de réponse valide, le service portail DOIT effectuer les opérations suivantes, non nécessairement dans cet ordre:

- mettre la valeur de l'objet cabhPsDevTodSyncStatus à "2" (échec d'accès au serveur ToD);
- s'il y a des connexions louées actives dans le secteur LAN-Trans comme indiqué par une valeur différente de zéro pour cabhCdpLanTransCurCount, mettre l'objet cabhCdpLanAddrCreateTime à l'heure actuelle et mettre l'objet cabhCdpLanAddrExpireTime à la valeur de l'objet cabhCdpLanAddrCreateTime plus la valeur de l'objet cabhCdpServerLeaseTime pour chaque location active (heure d'expiration = heure de création + temps de location);
- enregistrer l'échec et générer un événement normalisé défini en Annexe B;
- continuer de réessayer les communications avec le serveur temporel jusqu'à l'établissement de l'heure locale;
- essayer de télécharger le fichier de configuration PS comme décrit au § 7.3.3.2.

Si le serveur temporel renvoie effectivement une réponse valide, le service portail DOIT effectuer les opérations suivantes, non nécessairement dans cet ordre:

- mettre la valeur de l'objet cabhPsDevTodSyncStatus à "1" (succès d'accès au serveur ToD);
- s'il y a des connexions louées actives dans le secteur LAN-Trans comme indiqué par une valeur différente de zéro pour l'objet cabhCdpLanTransCurCount, mettre l'objet cabhCdpLanAddrCreateTime à l'heure actuelle et mettre l'objet cabhCdpLanAddrExpireTime à la valeur de l'objet cabhCdpLanAddrCreateTime plus la valeur de l'objet cabhCdpServerLeaseTime pour chaque location active (heure d'expiration = heure de création + temps de location);
- essayer de télécharger le fichier de configuration PS comme décrit au § 7.3.3.2.

Si la valeur de l'objet cabhPsDevTodSyncStatus est "1", c'est-à-dire si l'heure locale a déjà été établie, il n'est pas nécessaire que le client d'heure actuelle envoie une demande d'heure.

Le service PS ne DOIT envoyer et recevoir des messages ToD que par l'intermédiaire d'une interface WAN-Man.

8 Traitement de paquet et traduction d'adresse

8.1 Introduction/Aperçu général

8.1.1 Objectifs

Les objectifs clés qui régissent les capacités de traitement de paquet dans l'environnement IPCable2Home sont les suivants:

- fournir une fonction de traduction d'adresse facile sur le câble, offrant au câblo-opérateur la visibilité et la facilité de gestion des dispositifs de l'utilisateur tout en préservant les architectures d'acheminement fondées sur une ressource de réseau câblé;
- empêcher le trafic inutile sur le réseau câblé et sur le réseau du domicile;
- conserver les adresses IP acheminables mondialement ainsi que les adresses de gestion privée de réseau câblé;
- faciliter l'acheminement du trafic IP résidentiel en attribuant des adresses de réseau aux dispositifs IP de réseau LAN de telle sorte qu'ils résident dans le même sous-réseau logique.

8.1.2 Hypothèses

- on suppose que, lorsque les serveurs d'approvisionnement de câblo-opérateur fournissent de multiples adresses IP acheminables mondialement aux dispositifs résidentiels des clients, ces adresses ne résideront pas nécessairement dans le même sous-réseau;
- le changement de fournisseurs de service Internet est supposé ne survenir qu'assez rarement, à un rythme similaire à celui du changement de transporteur primaire à longue distance par un abonné résidentiel;

8.2 Architecture

Le présent paragraphe décrit les concepts clés de la fonction de traitement de paquet et de traduction d'adresse dans l'environnement IPCable2Home.

8.2.1 Directives pour la conception du système

Tableau 8-1/J.191 – Directives pour la conception d'un système de traitement de paquet et de traduction d'adresse

Numéro	Directives pour la conception du système
Traitement de paquet 1	Les mécanismes d'adressage seront sous le contrôle de l'opérateur et permettront à celui-ci d'en avoir connaissance et d'accéder aux dispositifs IPCable2Home.
Traitement de paquet 2	L'adressage ne fera rien qui puisse compromettre les architectures actuelles d'acheminement du réseau câblé (par exemple, l'acheminement fondé sur la source, par commutation MPLS).
Traitement de paquet 3	Les mécanismes de gestion du trafic isoleront le réseau câblé du trafic généré par les communications résidentielles d'homologue à homologue, s'il y a lieu.
Traitement de paquet 4	Les adresses IP seront conservées lorsque ce sera possible (à la fois les adresses acheminables mondialement et les adresses de gestion privée du réseau câblé).

8.2.2 Description du système de traitement de paquet

Le présent paragraphe donne un aperçu général des concepts de traitement de paquet et de traduction d'adresse.

8.2.2.1 Aperçu général de la fonction de traitement de paquet

La fonction de traduction d'adresse et de traitement de paquet est fournie par l'entité fonctionnelle appelée *portail d'adresse câble* (CAP), qui englobe les éléments suivants de traduction d'adresse et de transmission de paquet:

- traduction d'adresse câble (CAT);
- fonction de traversée;
- commutation de transmission sélective de sens montant (USFS).

Comme indiqué à la Figure 8-1, la fonction de traduction CAT fournit un mécanisme d'interconnexion des secteurs d'adresses WAN-Data et LAN-Trans (par traduction d'adresse), tandis que la fonction de traversée fournit un mécanisme d'interconnexion des secteurs d'adresses WAN-Data et LAN-Pass (par dérivation). La fonction de traduction CAT est conforme à la traduction d'adresse de réseau (NAT) traditionnelle de la section 2 du document RFC 3022. Comme avec la traduction NAT traditionnelle, il y a deux variantes de traduction CAT, dites *acheminement transparent de traduction d'adresse de réseau câblé* (C-NAT) et *acheminement transparent de traduction d'adresse et de point d'accès de réseau câblé* (C-NAPT). L'acheminement transparent C-NAT est la version conforme au réseau câblé de la traduction NAT de base de la section 2.1 du document RFC 3022 et l'acheminement transparent C-NAPT est la version conforme au réseau câblé de la traduction NAPT de la section 2.2 du document RFC 3022.

Selon le document RFC 3022, l'acheminement transparent C-NAT est "une méthode de mappage des adresses IP d'un groupe à un autre, transparente aux utilisateurs finals", et l'acheminement transparent C-NAPT est "une méthode par laquelle de nombreuses adresses de réseau et leurs points d'accès TCP/UDP (protocole de commande de transmission/protocole datagramme d'utilisateur) sont converties en une seule adresse de couche Réseau avec ses points d'accès TCP/UDP". Aussi, selon le document RFC 3022, l'objet des fonctions C-NAT et C-NAPT est de "fournir un mécanisme de connexion d'un secteur d'adresses privées à un secteur externe ayant des adresses mondiales enregistrées de façon unique".

La fonction de traversée est un processus de dérivation spécifié qui interconnecte les secteurs d'adresses WAN-Data et LAN-Pass sans traduction d'adresse.

La commutation de transmission sélective de sens montant (USFS) définit au sein du portail CAP une fonction qui a la capacité de confiner le trafic résidentiel dans le réseau du domicile, même lorsque les dispositifs d'utilisateur qui génèrent ce trafic résident dans des sous-réseaux logiques IP différents. Spécifiquement, cette fonction retransmet directement à sa destination le trafic qui provient d'une adresse située dans un des secteurs d'adresses du réseau LAN et qui est destiné à des secteurs d'adresses IP de réseau LAN. Cette fonction de retransmission directe empêche le trafic de traverser le réseau HFC, et interconnecte les secteurs d'adresses LAN-Trans et LAN-Pass.

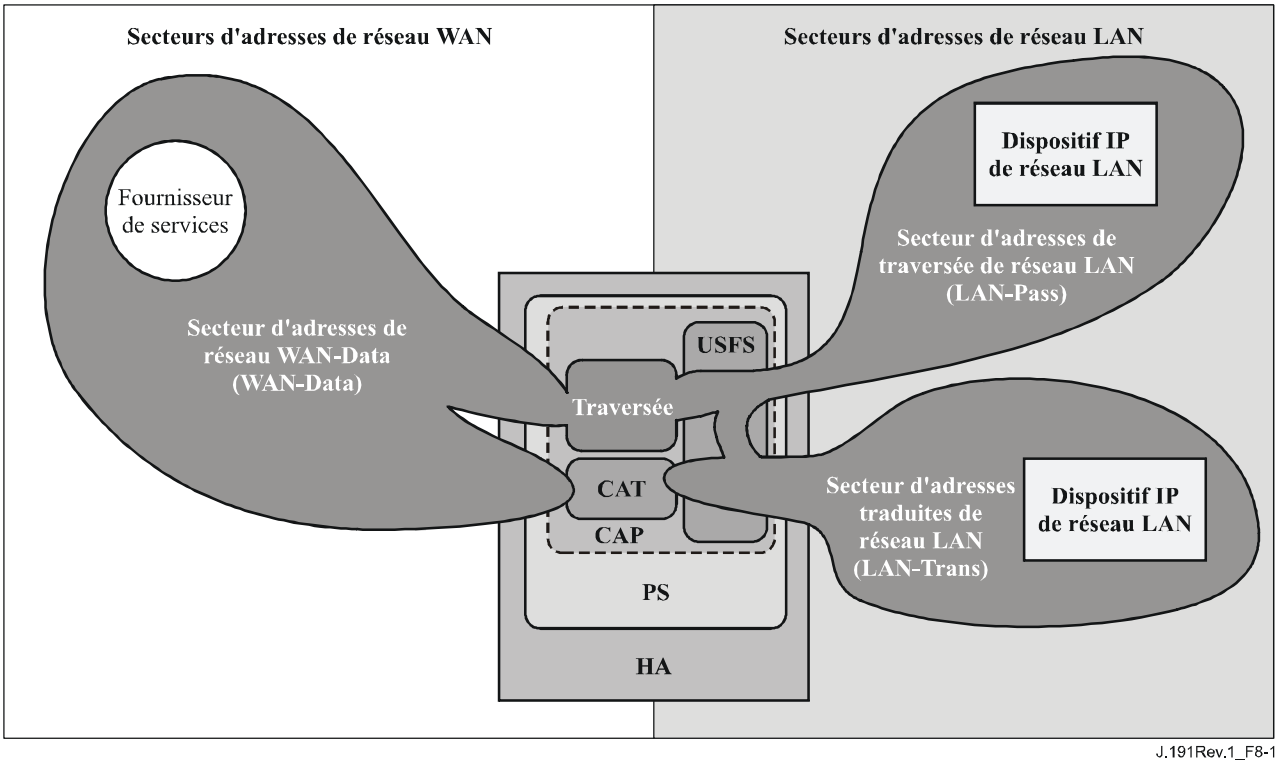


Figure 8-1/J.191 – Fonctions du portail d'adresse câble (CAP)

Tout au long de la présente Recommandation, les termes de *liaison d'adresse, non-liaison d'adresse, traduction d'adresse* et *session* sont utilisés selon les définitions du document RFC 2663. De plus, le terme *mappage* est défini comme étant l'information nécessaire pour effectuer l'acheminement transparent C-NAT et l'acheminement transparent C-NAPT.

En particulier, un mappage C-NAT est défini comme un nuplet de la forme (adresse IP de réseau WAN-Data, adresse IP de réseau LAN-Trans) fournissant un mappage bi-univoque entre les adresses WAN-Data et les adresses LAN-Trans. De même, un mappage C-NAPT est défini comme un nuplet de la forme (adresse IP de réseau WAN-Data et point d'accès TCP/UDP, adresse IP de réseau LAN-Trans et point d'accès TCP/UDP) fournissant un mappage multivoque entre une adresse WAN-Data unique et des adresses LAN-Trans multiples. Pour le trafic en protocole ICMP (comme une validation par écho), on utilise un numéro de séquence ICMP à la place du numéro de point d'accès TCP/UDP.

Le trafic de réseau LAN à réseau WAN est défini comme étant formé de paquets issus de dispositifs IP de réseau LAN et destinés à des dispositifs situés du côté WAN du service portail. Le trafic de réseau WAN à réseau LAN est défini comme étant formé de paquets issus de serveurs WAN et destinés à des dispositifs IP de réseau LAN. Le trafic de réseau LAN à réseau LAN est défini comme étant des paquets issus de dispositifs IP de réseau LAN et destinés à des dispositifs IP de réseau LAN situés dans le même sous-réseau ou dans un sous-réseau différent.

8.2.2.2 Modes de traitement des paquets

L'élément de services PS est configurable au moyen de l'objet de base MIB cabhCapPrimaryMode, afin de fonctionner dans un des trois modes primaires de traitement de paquet lors du traitement de trafic de réseau LAN à réseau WAN et de réseau WAN à réseau LAN: mode de traversée, mode d'acheminement transparent C-NAT, mode d'acheminement transparent C-NAPT. De plus, les modes primaires C-NAT ou C-NAPT peuvent aussi fonctionner dans un mode mixte décrit ci-dessous.

En mode de traversée, le portail CAP agit comme un pont transparent [ISO/CEI 15802-3] entre le secteur WAN-Data et le secteur LAN-Pass. En mode de traversée, les décisions de retransmission sont d'abord prises dans la couche 2 de l'OSI (couche Liaison de données). Dans ce mode, le portail CAP n'accomplit aucune fonction d'acheminement transparent C-NAT ou C-NAPT.

Le portail CAP accepte la transmission de couche 3 de l'OSI (couche Réseau) à la fois dans le mode d'acheminement transparent C-NAT et dans le mode d'acheminement transparent C-NAPT, décrits ci-dessous.

En mode C-NAT, l'élément de services PS (client CDC) acquiert une ou plusieurs adresses IP utilisées pour le trafic WAN-Data pendant le processus d'amorçage du service portail. Après acquisition par protocole DHCP, ces adresses IP sont utilisées comme portion d'adresses IP de réseau WAN-Data des nuplets de mappage C-NAT créés dynamiquement. S'il existe des adresses IP disponibles dans la réserve d'adresses IP de réseau WAN-Data, le portail CAP crée un mappage dynamique C-NAT lorsqu'il détecte pour la première fois du trafic IP de réseau LAN à réseau WAN qui n'a pas de mappage existant. S'il n'existe pas d'adresses IP disponibles dans la réserve d'adresses IP de réseau WAN-Data, le mappage dynamique C-NAT ne peut pas être créé, ce trafic est abandonné, et un événement est produit (voir Annexe B).

La portion d'adresses IP de réseau LAN-Trans des nuplets de mappage C-NAT créés dynamiquement est fournie par la réserve d'adresses IP définie par le câblo-opérateur dans la base MIB du portail CDP. Le portail CAP introduit le nuplet de l'unique adresse IP de réseau WAN-Data ainsi qu'une unique adresse IP de réseau LAN-Trans dans la table de mappage du portail CAP, de même que d'autres paramètres dont les numéros des points d'accès WAN et LAN, la méthode de mappage et le protocole de transport utilisé pour le mappage. Le numéro de point d'accès ne sera pas converti par le portail CAP pour les mappages de traduction C-NAT: les numéros de point d'accès de source et de destination contenus dans l'en-tête UDP ou TCP seront conservés sans changement. Le portail CAP introduit la valeur 0 dans les entrées correspondant aux points d'accès WAN et LAN de la table de mappage du portail CAP. L'entrée correspondant au point d'accès numéro zéro aura deux fonctions:

1) indiquer au portail CAP que les numéros de point d'accès ne doivent pas être convertis;
2) indiquer à tout lecteur de la table de mappage du portail CAP qu'il s'agit d'un mappage de traduction C-NAT, assurant ainsi la distinction entre mappages C-NAT (point d'accès de numéro 0) et mappages C-NAPT (point d'accès de numéro différent de zéro).

Les mappages dynamiques C-NAT pour le trafic UDP sont détruits lorsqu'une temporisation de période d'inactivité, cabhCapUdpTimeWait, arrive à expiration. Les mappages dynamiques C-NAT pour le trafic TCP sont détruits lorsqu'une temporisation de période d'inactivité, cabhCapTcpTimeWait, arrive à expiration ou qu'une session TCP se termine. Les mappages dynamiques C-NAT pour le trafic ICMP sont détruits lorsqu'une temporisation de période d'inactivité, cabhCapIcmpTimeWait, arrive à expiration. De plus, les mappages statiques C-NAT peuvent être créés ou détruits lorsque le système NMS écrit ou supprime des entrées de la table de base MIB cabhCapMappingTable.

En mode C-NAPT (mode de construction par défaut pour le système) l'élément de services PS (client CDC) acquiert une adresse IP, utilisée pour le trafic WAN-Data. Après acquisition par protocole DHCP, cette adresse IP est utilisée comme portion d'adresse IP de réseau WAN-Data des nuplets de mappage C-NAPT créés dynamiquement. Si l'adresse IP de réseau WAN-Data a été acquise, les mappages dynamiques C-NAPT sont créés lorsque le portail CAP détecte pour la première fois du trafic de réseau LAN à réseau WAN qui n'a pas de mappage existant. Si l'adresse IP de réseau WAN-Data n'a pas été acquise (c'est-à-dire qu'il n'y a pas de location DHCP active), le mappage dynamique C-NAPT ne peut pas être créé, ce trafic est abandonné, et un événement normalisé est généré (voir Annexe B).

Les mappages dynamiques C-NAPT pour le trafic UDP sont détruits lorsqu'une temporisation de période d'inactivité, cabhCapUdpTimeWait, arrive à expiration. Les mappages dynamiques C-NAPT pour le trafic TCP sont détruits lorsqu'une temporisation de période d'inactivité, cabhCapTcpTimeWait, arrive à expiration ou qu'une session TCP se termine. Les mappages dynamiques C-NAPT pour le trafic ICMP sont détruits lorsqu'une temporisation de période d'inactivité, cabhCapIcmpTimeWait, arrive à expiration. De plus, des mappages statiques C-NAPT peuvent être créés ou détruits lorsque le système NMS écrit ou supprime des entrées dans la table de base MIB cabhCapMappingTable.

La Figure 8-2 montre un processus typique de mappage dynamique C-NAPT avec un paquet TCP. Dans cet exemple, le service portail est configuré pour fonctionner en mode NAPT et a déjà obtenu une adresse IP de réseau WAN, tandis que le dispositif IP de réseau LAN a déjà obtenu une adresse IP dans le secteur LAN-Trans.

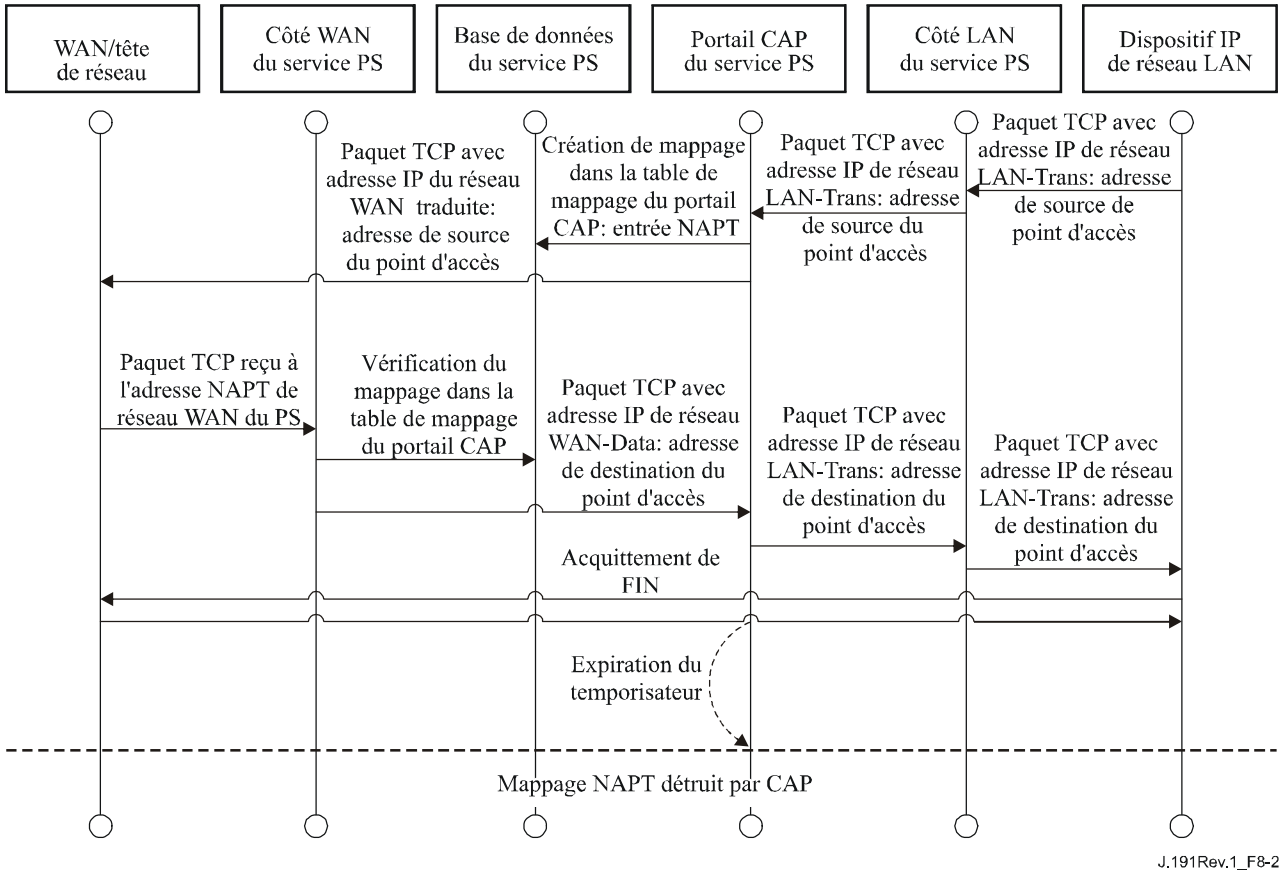


Figure 8-2/J.191 – Diagramme séquentiel de configuration du service PS (table de mappage CAP – NAPT)

Le service portail peut également fonctionner en mode mixte de dérivation/acheminement. Dans ce cas, le système NMS règle le mode primaire à l'acheminement transparent C-NAT ou C-NAPT, et le système NMS écrit dans la table de traversée une ou plusieurs adresses MAC appartenant aux dispositifs IP de réseau LAN dont le trafic doit être ponté (objet cabhCapPassthroughTable). Dans ce mode mixte, le service portail examine les adresses MAC des trames reçues pour déterminer s'il faut dériver la trame en transparence ou appliquer d'éventuelles fonctions d'acheminement transparent C-NAT ou C-NAPT dans la couche IP. Dans le cas du trafic de réseau LAN à réseau WAN, le service portail examine l'adresse de commande MAC source et, si cette adresse de commande MAC existe dans la table cabhCapPassthroughTable, la trame est pontée de façon transparente vers l'interface WAN-Data. Dans le cas de trafic de réseau WAN à LAN, le service portail examine l'adresse de commande MAC de destination et, si cette adresse de commande MAC existe dans la table cabhCapPassthroughTable, la trame est pontée de façon transparente vers l'interface LAN appropriée. Si l'adresse de commande MAC n'existe pas dans la table cabhCapPassthroughTable, le paquet est traité par des fonctions de couches supérieures, y compris la fonction d'acheminement transparent C-NAT/C-NAPT.

L'on part du principe que, lorsque le service PS est en mode d'acheminement (C-NAT/C-NAPT), il traite le trafic diffusé conformément aux documents RFC 919, 922, 1812 et 2644. L'on part également du principe que, lorsque le service PS est en mode de traversée, le trafic diffusé est ponté vers toutes les interfaces.

Lorsque le service PS est en mode mixte de dérivation/acheminement et qu'il reçoit du trafic diffusé en provenance d'un dispositif figurant dans la table de traversée, le service PS est censé dériver ce trafic diffusé vers toutes les interfaces. Lorsque le service PS est en mode mixte de dérivation/acheminement et qu'il reçoit du trafic diffusé sur une quelconque interface WAN, le service PS est censé dériver ce trafic diffusé vers toutes les interfaces LAN.

Il faut noter que la fonctionnalité de commutation USFS (voir § 8.2.2.3) est appliquée dans chacun des trois modes primaires de traitement de paquet sans que l'utilisation ou non du mode mixte entre en considération. Les décisions de retransmission par commutation USFS prendront le pas sur les autres décisions de retransmission qui pourraient éventuellement retransmettre du trafic du réseau LAN vers le réseau WAN.

8.2.2.3 Généralités sur la commutation de transmission sélective de sens montant

Dans certains cas, un dispositif IP de secteur d'adresses LAN-Pass résidera dans un sous-réseau IP logique différent de celui des autres dispositifs IP de réseau LAN connectés au même élément de services PS. Il importe d'empêcher le trafic entre ces dispositifs IP de réseau LAN de traverser le réseau HFC: empêcher ce trafic HFC non désiré est la fonction qui est fournie par la commutation de transmission sélective de sens montant (USFS).

Spécifiquement, la fonction USFS achemine le trafic – qui prend son origine dans le réseau du domicile et qui est destiné à ce réseau – directement à sa destination. Le trafic provenant d'un dispositif IP de réseau LAN dont l'adresse IP de destination est en dehors du secteur d'adresses du réseau LAN est transmis sans altération à la fonction de dérivation/acheminement du portail CAP.

La fonctionnalité USFS utilise la table de traduction d'adresse IP (comme définie dans RFC 2011) au sein de l'élément de services PS. Cette table – ipNetToMediaTable – du document RFC 2011 contient une liste d'adresses MAC, leurs adresses IP correspondantes, et les numéros d'indice d'interface de services portail auxquels ces adresses sont associées. La fonction USFS va se référer à cette table afin de prendre des décisions sur la façon de diriger le flux de trafic de réseau LAN vers WAN. Pour remplir la table ipNetToMediaTable, le service portail apprend les adresses IP et MAC et leurs associations. Pour chaque interface physique associée, le service portail apprend toutes les adresses IP de réseau LAN-Trans et LAN-Pass avec leurs liaisons MAC associées. Cet apprentissage peut se faire via différentes méthodes. Les méthodes d'apprentissage d'adresse IP/MAC spécifiques du vendeur peuvent inclure: l'espionnage du portail ARP, la surveillance du

trafic, et la consultation des entrées de portail CDP. Les entrées sont purgées de la table ipNetToMediaTable après l'expiration d'une période raisonnable de temporisation d'inactivité.

La fonction de commutation USFS inspecte tout le trafic IP reçu sur les interfaces LAN du service portail. Si l'adresse IP de destination se trouve (via la table ipNetToMediaTable) résider sur une interface LAN de services portail, l'adresse de destination de couche de liaison de données de la trame originale est changée de façon à passer de l'adresse de la passerelle par défaut à celle du dispositif IP de réseau LAN de destination et le trafic est retransmis sur l'interface LAN de services portail appropriée. Si l'on ne trouve pas de correspondance avec l'adresse IP de destination dans la table ipNetToMediaTable, le paquet est transmis, dans sa forme originale, à la fonction d'acheminement transparent C-NAT/C-NAPT ou à la fonction de dérivation de traversée (selon le mode de traitement de paquet activé).

8.2.2.4 Multidiffusion

Le portail CAP accepte le trafic multidiffusé par la dérivation transparente des messages IGMP en aval (selon RFC 2236) et des paquets IP multidiffusés en aval. Par ailleurs, lorsqu'il est en mode d'acheminement transparent C-NAT/C-NAPT, le portail CAP effectue la traduction d'adresse dans les messages IGMP amont provenant de dispositifs IP de réseau LAN résidant dans le domaine LAN-Trans. Le portail CAP retransmet vers le réseau LAN le trafic IGMP provenant du réseau WAN afin que les notifications puissent atteindre les dispositifs IP de réseau LAN. Un dispositif IP de réseau LAN va déterminer à quelle multidiffusion il souhaite se joindre et va envoyer un message multidiffusé "d'entrée en participation". La source multidiffusée sera alors capable de transmettre des données au dispositif IP de réseau LAN. Lorsque le service multidiffusé n'est plus désiré, le dispositif IP de réseau LAN peut soit ignorer ce service dont le flux s'arrêtera en fin de temporisation, ou envoyer un message IGMP de "sortie de participation" à la chaîne afin de libérer le flux de trafic. La Figure 8-3 donne un exemple détaillé des processus IGMP et multidiffusés passant à travers un service portail.

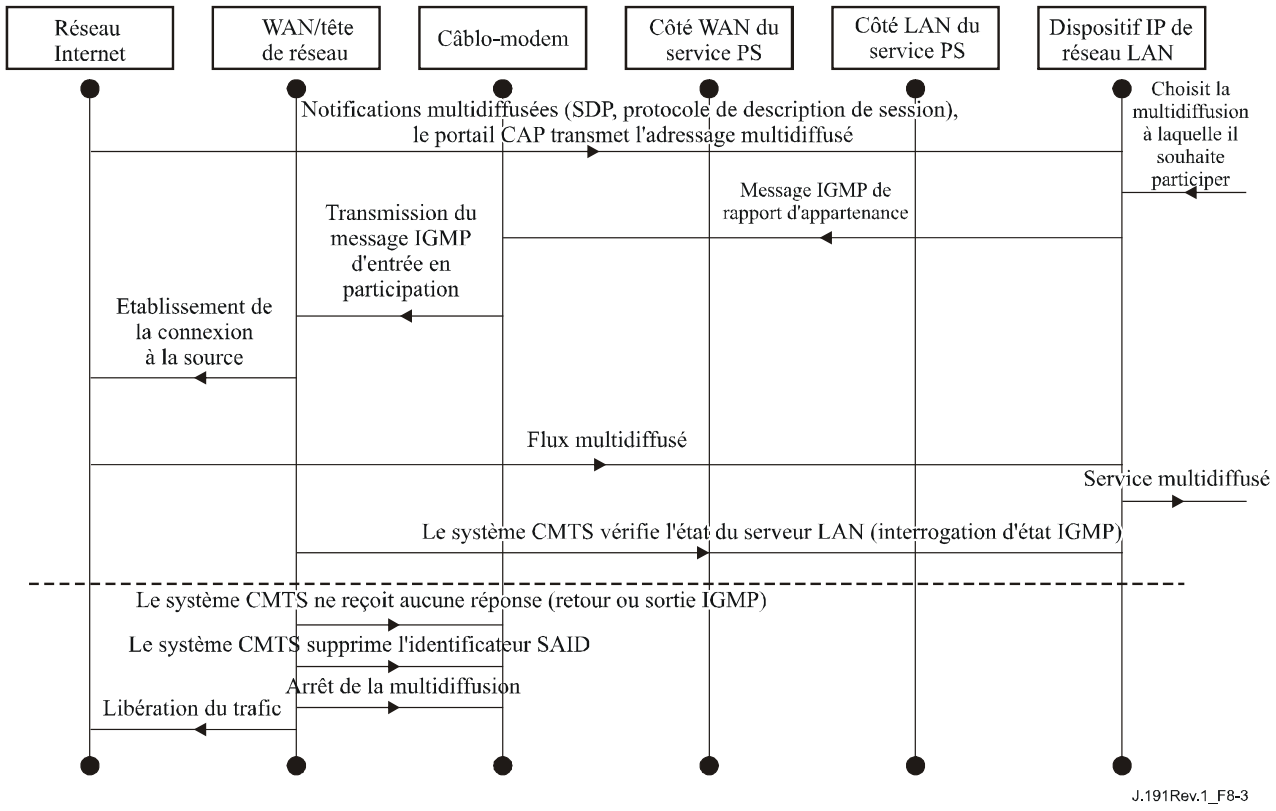


Figure 8-3/J.191 – Multidiffusion via une séquence IGMP

8.2.2.5 Exemples de traitement de paquet

Le présent paragraphe donne quelques informations sur les processus impliqués dans le traitement de paquet. La Figure 8-4 donne un exemple d'étapes possibles de traitement de paquet pour le trafic unidiffusé de réseau LAN à réseau WAN, et la Figure 8-5 donne un exemple d'étapes possibles de traitement de paquet pour du trafic unidiffusé de réseau WAN à réseau LAN. Ces exemples ne sont qu'informatifs et n'impliquent aucune obligation quant à l'implémentation.

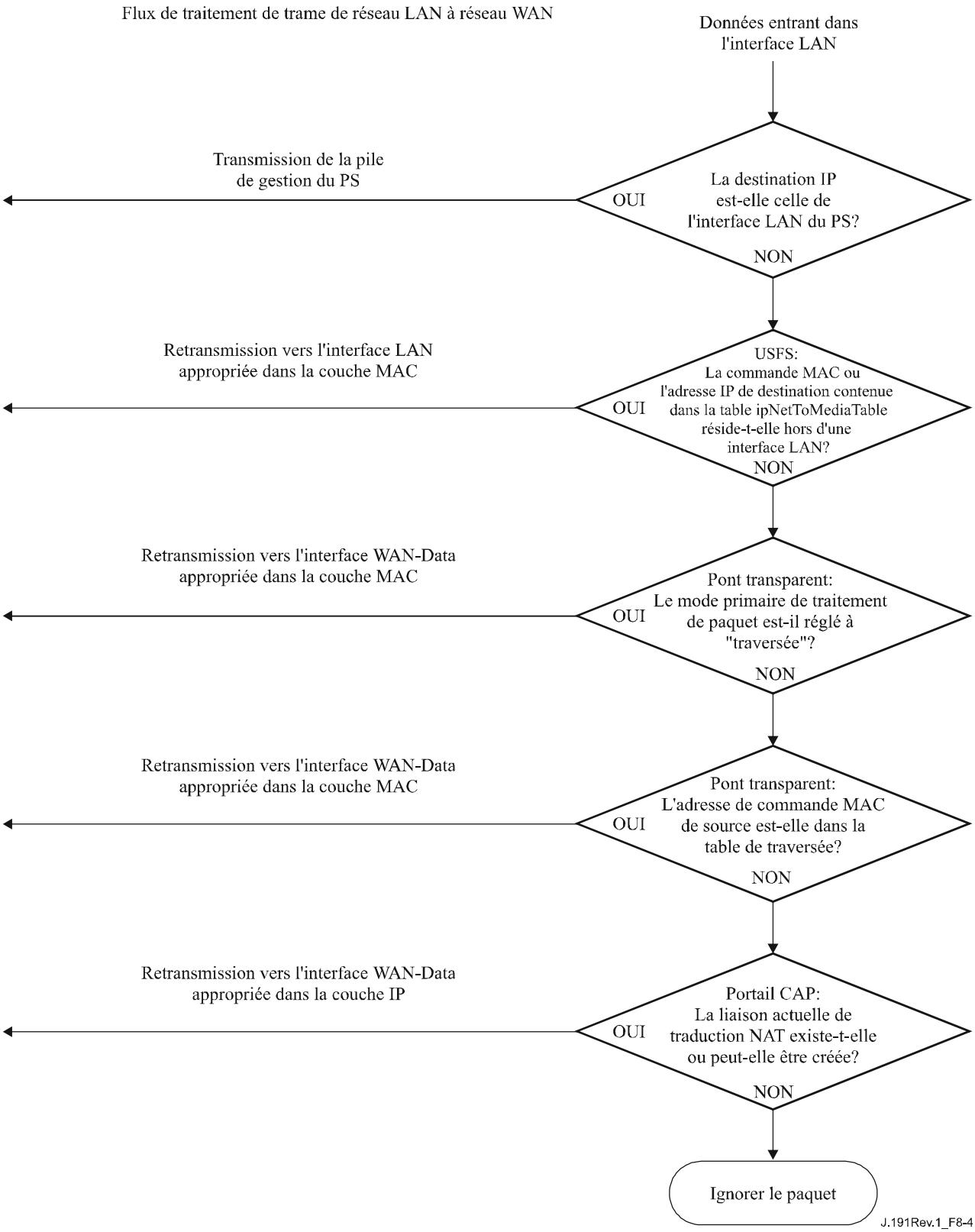


Figure 8-4/J.191 – Exemple de traitement de paquet de réseau LAN à réseau WAN

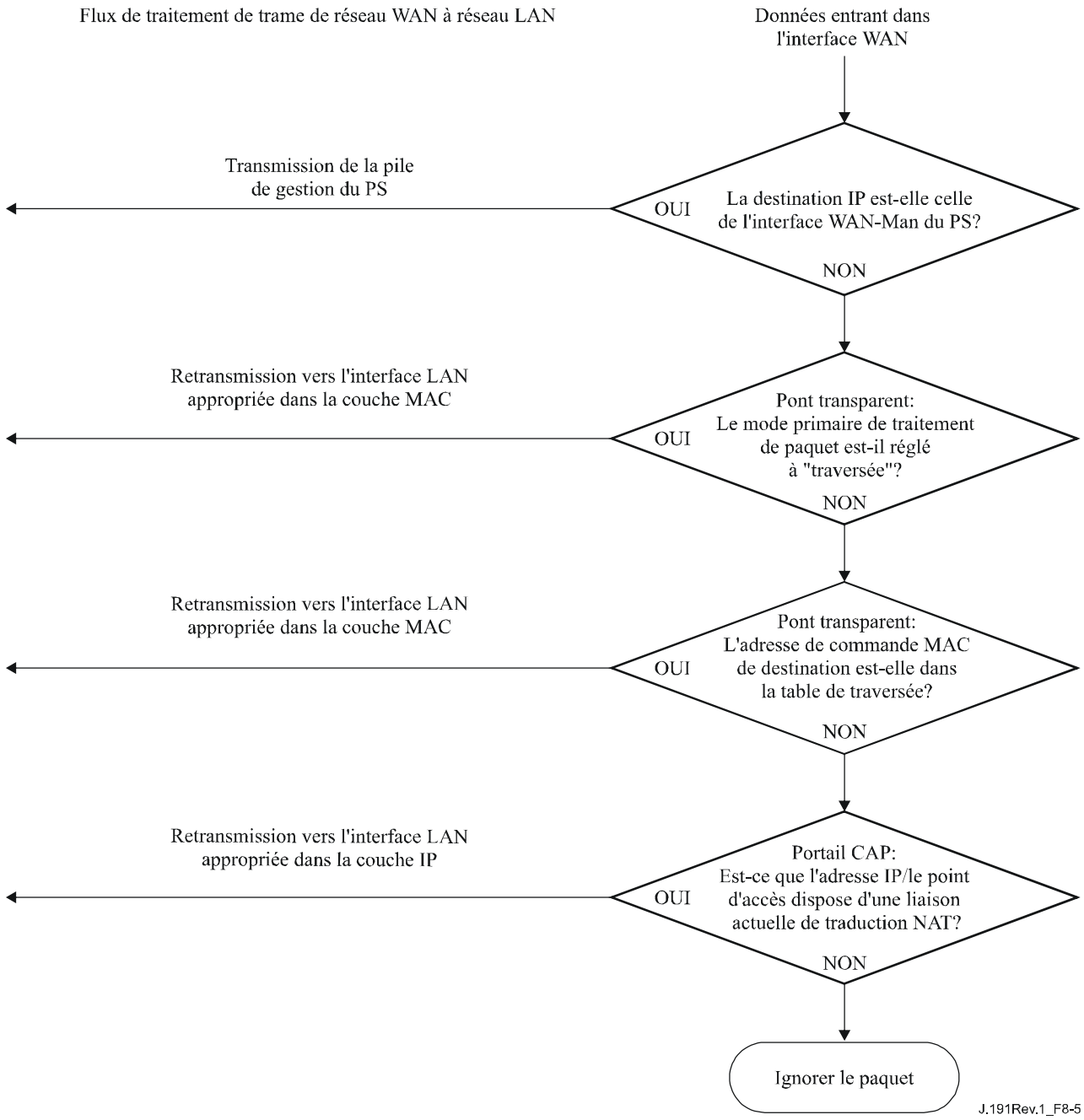


Figure 8-5/J.191 – Exemple de traitement de paquet de réseau WAN à réseau LAN

8.3 Exigences relatives au portail CAP

8.3.1 Exigences générales

Toutes les interfaces IP logiques avec l'élément de services PS DOIVENT être conformes aux sections 3 et 4 du document RFC 1122, afin de permettre des communications normalisées avec les serveurs Internet.

Le portail CAP DOIT prendre en charge le trafic multidiffusé de réseau WAN à réseau LAN, au moyen de la dérivation transparente de messages IGMP et de paquets multidiffusés IP de réseau WAN à réseau LAN comme défini dans RFC 2236.

Si le mode primaire de traitement de paquet, objet cabhCapPrimaryMode, est réglé à 'traversée', tous les messages IGMP de réseau LAN à réseau WAN DOIVENT être pontés en transparence.

Si le mode primaire de traitement de paquet, objet cabhCapPrimaryMode, est réglé à C-NAPT, l'adresse IP de source de tous les messages IGMP de réseau LAN à réseau WAN, provenant de dispositifs IP de réseau LAN résidant dans le domaine LAN-Trans, DOIT être traduite en l'adresse IP de réseau WAN-Data utilisée pour les mappages de traduction C-NAPT puis être réexpédiée à l'extérieur du réseau WAN.

Si le mode primaire de traitement de paquet, objet cabhCapPrimaryMode, est réglé à C-NAT, l'adresse IP de source de tous les messages IGMP de réseau LAN à réseau WAN, provenant de dispositifs IP de réseau LAN résidant dans le domaine LAN-Trans, DOIT être traduite en l'adresse IP de réseau WAN-Data utilisée pour les mappages de traduction C-NAT puis être réexpédiée à l'extérieur du réseau WAN.

8.3.2 Exigences relatives au traitement des paquets

Le portail CAP DOIT prendre en charge le mode de traversée, le mode d'acheminement transparent C-NAT, et le mode d'acheminement transparent C-NAPT. Le portail CAP DOIT également prendre en charge la sélection de ce mode primaire de traitement de paquet, via l'objet de base MIB cabhCapPrimaryMode.

Si le mode primaire de traitement de paquet, objet cabhCapPrimaryMode, est réglé à C-NAT, le portail CAP DOIT s'assurer qu'il existe une adresse IP disponible, fournie par la tête de réseau dans la réserve d'adresses IP de réseau WAN-Data (avec une location DHCP en cours) avant d'essayer d'utiliser cette adresse IP comme partie d'un mappage C-NAT. Si le portail CAP n'est pas en mesure de créer un mappage C-NAT du fait de la réduction de la réserve d'adresses IP de réseau Wan-Data, ce portail doit générer un événement normalisé (comme défini à l'Annexe B).

Pour chaque mappage dynamique C-NAT qu'il crée, le portail CAP DOIT donner une valeur égale à zéro aux numéros de point d'accès WAN et LAN (objets cabhCapMappingWanPort et cabhCapMappingLanPort, respectivement) dans la table de mappage du portail CAP.

Si le câblo-opérateur crée ou modifie une rangée dans la table de mappage du portail CAP, c'est-à-dire si une rangée est créée par la méthode de mappage statique (cabhCapMappingMethod=static(1)) ET si les objets de point d'accès (cabhCapMappingLanPort et cabhCapMappingWanPort) ne sont pas spécifiés dans cette rangée, le portail CAP DOIT insérer dans cette rangée la valeur zéro pour les deux objets cabhCapMappingLanPort et cabhCapMappingWanPort.

Le portail CAP NE DOIT PAS convertir le numéro de point d'accès d'un paquet dont l'adresse IP apparaît dans la table de mappage du portail CAP avec un numéro de point d'accès égal à zéro.

Si le mode primaire de traitement de paquet, cabhCapPrimaryMode, est réglé à C-NAPT, le portail CAP DOIT s'assurer qu'il existe une adresse IP de réseau WAN en cours (avec une location DHCP en cours venant de l'approvisionnement de la tête de réseau) avant d'essayer d'utiliser cette adresse IP comme partie d'un mappage C-NAPT. Si le portail CAP n'est pas en mesure de créer un mappage C-NAPT du fait qu'il n'a pas d'adresse IP de réseau WAN en cours ou du fait de la réduction du nombre de points d'accès, ce portail DOIT générer un événement normalisé (comme défini à l'Annexe B).

Le trafic de réseau LAN à réseau LAN NE DOIT PAS être acheminé ou ponté hors d'une interface de réseau WAN.

Lorsque la location DHCP d'une adresse IP de réseau WAN-Data – faisant partie du mappage de traduction C-NAT ou C-NAPT – arrive à expiration, tous les mappages associés à cette adresse IP DOIVENT être supprimés de la table cabhCapMappingTable.

8.3.2.1 Exigences de traversée

Lorsque le mode primaire de traitement de paquet du portail CAP, cabhCapPrimaryMode, est réglé au mode de traversée, le portail CAP DOIT agir comme un pont transparent, comme défini dans

l'ISO/CEI 15802-3, entre le secteur WAN-Data et le secteur LAN-Pass, et NE DOIT PAS effectuer de fonctions d'acheminement transparent C-NAT ou C-NAPT. Même lorsque le mode primaire de traitement de paquet est réglé à 'traversée', le traitement de fonction USFS DOIT prendre le pas sur les décisions de dérivation de réseau LAN à réseau WAN.

8.3.2.2 Exigences d'acheminement transparent C-NAT et C-NAPT

Lorsque le mode primaire de traitement de paquet (objet cabhCapPrimaryMode) est réglé à C-NAT, le portail CAP DOIT accepter les processus de traduction d'adresse C-NAT conformément aux exigences de base de traduction NAT définies dans RFC 3022.

Lorsque le mode primaire de traitement de paquet (objet cabhCapPrimaryMode) est réglé à C-NAPT, le portail CAP DOIT accepter les processus de traduction d'adresse C-NAPT conformément aux exigences de base de traduction NAPT définies dans RFC 3022.

Sans considération du mode primaire de traitement de paquet, le portail CAP DOIT accepter la création et la suppression des mappages statiques de traduction C-NAT et C-NAPT, en permettant au système NMS de lire, de créer et de supprimer (via le portail CMP) les entrées de mappage statique de portail CAP (objet cabhCapMappingTable).

Les mappages statiques C-NAT et C-NAPT créés par le système NMS DOIVENT persister au-delà des réamorçages du service portail.

Le portail CAP DOIT accepter la création de mappages de traduction dynamique C-NAT et C-NAPT, initialisés par trafic TCP, UDP ou ICMP de réseau LAN à réseau WAN. Le portail CAP DOIT permettre au système NMS de lire (via le portail CMP) les entrées de mappage dynamique du portail CAP (objet cabhCapMappingTable).

Le portail CAP DOIT accepter la suppression de mappages dynamiques C-NAT et C-NAPT si un mappage donné est associé à une session TCP ET que cette session TCP se termine OU que la temporisation d'inactivité TCP, cabhCapTcpTimeWait, pour ce mappage, arrive à expiration.

Le portail CAP DOIT accepter la suppression de mappages dynamiques C-NAT et C-NAPT si un mappage donné est associé à une session UDP ET que la temporisation d'inactivité UDP, cabhCapUdpTimeWait, pour ce mappage, arrive à expiration.

Le portail CAP DOIT accepter la suppression de mappages dynamiques C-NAT et C-NAPT si un mappage donné est associé à une session ICMP ET que la temporisation d'inactivité ICMP, cabhCapIcmpTimeWait, pour ce mappage, arrive à expiration.

Les mappages dynamiques C-NAT et C-NAPT NE DOIVENT PAS persister au-delà des réamorçages de services portail.

8.3.2.3 Exigences du mode mixte de dérivation/acheminement

Le portail CAP DOIT accepter le mode mixte de dérivation/acheminement comme décrit au § 8.2.2, où le mode primaire de traitement de paquet au portail CAP, cabhCapPrimaryMode, est réglé à "acheminement transparent C-NAT ou C-NAPT" et où le portail CAP va aussi dériver de façon transparente du trafic pour des adresses MAC particulières. Si le mode primaire de traitement de paquet du portail CAP, cabhCapPrimaryMode, est réglé sur l'acheminement transparent C-NAT ou C-NAPT ET que le système NMS ait écrit une adresse de commande MAC appartenant à un dispositif IP de réseau LAN situé dans la table cabhCapPassthroughTable, ce portail CAP DOIT dériver de façon transparente le trafic de réseau LAN à réseau WAN originaire de cette adresse de commande MAC, ainsi que le trafic de réseau WAN à réseau LAN destiné à cette adresse de commande MAC.

En mode mixte de dérivation/acheminement, comme décrit au § 8.2.2, la fonction USFS DOIT être appliquée à tout le trafic d'origine LAN reçu.

8.3.3 Exigences relatives à la commutation USFS

La fonctionnalité de commutation de transmission sélective de sens montant (USFS) DOIT être appliquée au traitement de paquet sans considération du mode de traitement de paquet du portail CAP (traversée, C-NAT, C-NAPT, ou dérivation/acheminement mixte).

L'élément de services PS DOIT apprendre toutes les adresses IP de réseau LAN-Trans, IP de réseau LAN-Pass, et MAC des dispositifs IP de réseau LAN, associées à chacune de ses interfaces de réseau physique actives. Les adresses IP et MAC apprises par l'élément de services PS et les numéros d'index d'interface physique de services portail DOIVENT être accessibles au système NMS (à travers le portail CMP) via la table ipNetToMediaTable du document RFC 2011. L'élément de services PS DOIT supprimer les entrées de la table ipNetToMediaTable, lorsqu'une temporisation d'inactivité arrive à expiration.

La fonction USFS DOIT inspecter tout le trafic IP prenant son origine sur les interfaces de réseau LAN du service portail, pour déterminer si l'adresse IP de destination d'un paquet est celle d'un dispositif résidant sur une interface de réseau LAN du service PS. Si l'adresse IP de destination contenue dans un paquet inspecté par la fonction USFS est celle d'un dispositif IP de réseau LAN résidant hors d'une interface LAN du service portail, la fonction USFS DOIT remplacer l'adresse de destination de la couche MAC, au sein de l'en-tête de couche 2 du paquet, par l'adresse de commande MAC du dispositif IP de réseau LAN de cette destination et transmettre la trame à l'interface LAN physique appropriée.

9 Résolution de nom

9.1 Introduction/Aperçu général

9.1.1 Objectifs

Les objectifs de la résolution de nom sont les suivants:

- fournir aux clients DNS situés au sein des dispositifs IP de réseau LAN le système de dénomination de domaine (DNS, *domain name system*) à partir d'un serveur du service portail, même pendant les coupures de connexion du câble;
- permettre aux abonnés de voir lex dispositifs locaux au moyen de noms de dispositifs ayant une signification intuitive plutôt qu'au moyen d'une adresse IP;
- fournir, au moyen d'interrogations récurrentes auprès de serveurs DNS, des réponses aux clients DNS de réseau LAN lors d'interrogations portant sur la résolution de noms de serveurs non locaux;
- fournir une récupération de service DNS facile lors du rétablissement de la connexité du câble après une coupure.

9.1.2 Hypothèses

Les hypothèses de fonctionnement des services de nommage sont les suivantes:

- le serveur DNS situé dans l'élément de services PS est le seul serveur DNS qui fait foi pour les dispositifs IP de réseau LAN situés dans le secteur LAN-Trans;
- l'élément de services PS ne fournira pas le service DNS aux dispositifs IP de réseau LAN situés dans le secteur LAN-Pass;
- si l'élément de services PS utilise des adresses WAN-Data multiples, les informations de serveur DNS de réseau WAN obtenues pendant le plus récent processus (DHCP) d'acquisition d'adresse WAN-Data seront utilisées.

9.2 Architecture

9.2.1 Directives pour la conception du système

Tableau 9-1/J.191 – Directives pour la conception du système de résolution de nom

Référence	Directives pour la conception du système
Résolution de nom 1	Fournir le service de dénomination de domaine (DNS) à partir d'un serveur situé dans le service portail aux clients DNS situés dans les dispositifs IP de réseau LAN, pour la résolution de nom des dispositifs IP de réseau LAN (indépendamment de l'état de la connexion WAN).
Résolution de nom 2	Fournir aux clients DNS situés dans des dispositifs IP de réseau LAN, au moyen d'interrogations récurrentes commençant par un serveur DNS de tête de réseau, des réponses aux interrogations portant sur la résolution de noms de serveurs non locaux.

9.2.2 Description du système

Le présent paragraphe donne un aperçu général sur les services de résolution de nom au sein de l'élément de services PS.

9.2.2.1 Aperçu général sur le fonctionnement de la résolution de nom

Le portail de nommage du câble (CNP, *cable naming portal*) est un service fonctionnant dans le service portail qui fournit un serveur DNS simple aux dispositifs IP de réseau LAN situés dans le secteur d'adresses LAN-Trans. Le portail CNP n'est pas utilisé par les dispositifs IP de réseau LAN situés dans le secteur d'adresses LAN-Pass, parce qu'ils seront servis directement par les serveurs DNS extérieurs au domicile.

Tous les dispositifs IP de réseau LAN situés dans le secteur LAN-Trans sont configurés par le portail CDP de façon à utiliser le portail CNP comme leur serveur de nom de domaine. Le service portail CNP situé dans le secteur LAN-Trans ne dépend pas de l'état de la connexion WAN. Le portail CNP effectue les tâches suivantes:

- résolution des noms de serveur pour les dispositifs IP de réseau LAN, en retournant leurs adresses IP correspondantes;
- renvoi des dispositifs IP de réseau LAN à des serveurs DNS extérieurs pour les questions qui ne peuvent être résolues via les informations de services portail locales. Cette action ne se produit que lorsque des informations de serveur DNS de réseau WAN sont disponibles dans le service portail. Autrement, le portail CNP retourne une erreur indiquant que le nom ne peut être résolu à ce moment.

Faire du portail CNP le serveur DNS primaire dans les locaux de l'utilisateur évite d'avoir à reconfigurer les dispositifs IP de réseau LAN lors d'un changement d'état de la connexion WAN. Cela permet aussi de changer l'attribution de serveur DNS extérieur sans reconfigurer le dispositif IP de réseau LAN.

9.2.2.2 Fonctionnement de la résolution de nom

Lorsqu'il est interrogé pour résoudre un nom de serveur, le portail CNP effectue le processus d'exploration qui est indiqué à la Figure 9-1. Le portail CNP répond aux interrogations initiales du service DNS normalisé [RFC 1035], dirigées vers l'adresse cabhCdpServerDnsAddress, pour toutes les explorations de noms. Il appartient au portail CNP d'envoyer des interrogations récurrentes à des serveurs DNS extérieurs – en commençant par la première entrée d'objet cabhCdpWanDnsServerIp contenue dans une table cabhCdpWanDnsServerTable lors d'une interrogation issue d'un dispositif IP de réseau LAN. Il lui appartient également de répondre à ce dispositif IP de réseau LAN, par un message de réponse ou d'erreur.

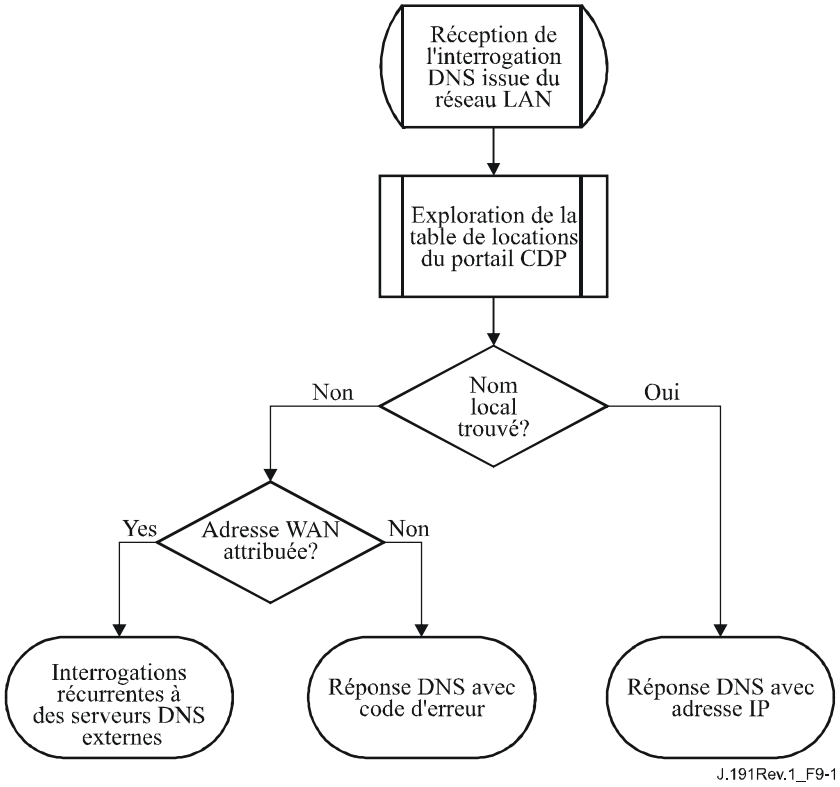


Figure 9-1/J.191 – Traitement de paquet au portail CNP

Le portail CNP se fonde sur la table cabhCdpLanAddrTable du portail CDP pour prendre connaissance des noms de serveur associés aux adresses IP actuelles des dispositifs IP de réseau LAN actifs. Tant que le dispositif IP de réseau LAN maintient une location DHCP active avec le portail CDP et a fourni un nom de serveur au portail CDP (au titre du processus d'acquisition de son adresse IP) son nom peut être résolu par le portail CNP. Si le nom de serveur dont la résolution est demandée ne peut pas être trouvé dans la table cabhCdpLanAddrTable, le portail CNP adresse des interrogations récurrentes à des serveurs DNS externes (dont le premier est obtenu par le client CDC au moyen d'options DHCP).

Une interrogation normale de serveur DNS spécifie un nom de domaine cible (QNAME), un type d'interrogation (QTYPE) et une classe d'interrogation (QCLASS). Elle demande des enregistrements de ressources qui correspondent. Le portail CNP répond aux interrogations de serveur DNS par les champs QCLASS = IN, QTYPE = A, NS, SOA ou PTR comme défini dans le document RFC 1035. La prise en charge des transferts de zone et du service DNS par protocole TCP n'est pas exigée.

Dans la mesure où le portail CNP est un serveur DNS autorisé dans le secteur LAN-Trans, ce portail va fournir sur demande les enregistrements de début d'autorité (SOA) et de serveur de nom (NS) autorisé. Le Tableau 9-2 est un exemple des champs d'enregistrement de début SOA (voir le § 3.3.13 du document RFC 1035):

Tableau 9-2/J.191 – Champs d'enregistrement SOA

Champ RDATA de RFC 1035	Objet MIB de portail CDP
MNAME	cabhCdpServerDomainName
RNAME	Non spécifié
SERIAL	Non spécifié
REFRESH	Non spécifié
RETRY	Non spécifié
EXPIRE	Non spécifié
MINIMUM	Non spécifié

Le champ MNAME est le nom de domaine du secteur d'adresses LAN-Trans. Le portail CNP utilise la valeur conservée dans l'objet cabhCdpServerDomainName comme nom de domaine du secteur d'adresses LAN-Trans.

La champ RNAME est la boîte à lettres de la personne responsable du domaine. Si le service portail conserve une adresse électronique pour un administrateur, ces informations pourront être spécifiées dans ce champ.

Le champ SERIAL est un nombre arithmétique de 32 bits, utilisé pour identifier la version des informations de zone. Mais dans la mesure où les transferts de zone ne sont pas spécifiés, la valeur de ce champ n'est pas spécifiée.

9.3 Exigences relatives à la résolution des noms

Le portail CNP DOIT être conforme au format de message DNS normalisé et accepter les interrogations DNS normalisées, comme décrit dans les documents RFC 1034 et RFC 1035.

Le portail CNP est un serveur sans état qui DOIT être capable de recevoir des interrogations et d'envoyer des réponses en paquets UDP [RFC 768].

Le portail CNP DOIT fonctionner au moins en mode non récurrent, comme défini dans RFC 1034.

Le portail CNP répond aux interrogations de nom en n'utilisant que des informations locales au sein du service portail et ses messages de réponse DOIVENT contenir une erreur ou une réponse.

Le portail CNP ne DOIT répondre qu'aux interrogations DNS adressées à l'adresse contenue dans l'objet cabhCdpServerDnsAddress.

Le portail CNP NE DOIT PAS répondre à des interrogations DNS envoyées aux adresses IP de réseau WAN-Man et PS/WAN-Data.

Dès réception d'une demande initiale de résolution de nom de serveur de la part d'un dispositif IP de réseau LAN, le portail CNP DOIT accéder à la table cabhCdpLanAddrTable du portail CDP afin d'examiner les noms de serveur associés aux adresses IP qui sont louées à des dispositifs IP de réseau LAN.

Sans considération de l'existence d'éventuelles entrées cabhCdpWanDnsServerIp dans la table cabhCdpWanDnsServerTable du portail CDP, si le nom de serveur peut être résolu par le portail CNP à partir de données locales, le portail CNP DOIT répondre à l'interrogation de résolution de nom de serveur par l'adresse IP du dispositif IP de réseau LAN nommé.

Si le nom de serveur demandé ne peut pas être résolu par le portail CNP à partir des données locales ET que la table cabhCdpWanDnsServerTable soit remplie avec au moins une entrée cabhCdpWanDnsServerIp, le portail CNP DOIT tenter de résoudre l'interrogation relative au nom de serveur au moyen d'interrogations récurrentes auprès de serveurs DNS externes, en commençant

par des interrogations adressées aux serveurs DNS représentés par l'entrée cabhCdpWanDnsServerIp dans la table cabhCdpWanDnsServerTable.

Si le nom de serveur ne peut pas être résolu par le portail CNP à partir de données locales ET qu'aucune entrée cabhCdpWanDnsServerIp n'existe dans la table cabhCdpWanDnsServerTable, le portail CNP DOIT répondre à l'interrogation relative à la résolution du nom de serveur par l'erreur appropriée qui est spécifiée par le document RFC 1035.

Le portail CNP DOIT répondre aux interrogations DNS du type QCLASS = IN, et du type QTYPE = A, NS, SOA ou PTR.

Les réponses du portail CNP aux interrogations DNS DOIVENT être conformes à la section 3.3 du document RFC 1035, avec le bit de réponse d'autorisation mis à "1" dans la section d'en-tête (voir la section 4.1.1 du document RFC 1035).

Etant donné que le portail CNP est un serveur DNS autorisé au sein du secteur LAN-Trans, il DOIT fournir sur demande les enregistrements de début d'autorité (SOA) et de serveur de nom (NS) autorisé. Les champs d'enregistrement de début SOA (voir la section 3.3.13 du document RFC 1035) DOIVENT contenir une entrée pour le champ MNAME qui soit égale à la valeur de l'objet de base MIB cabhCdpServerDomainName du portail CDP.

Si le nom cabhCdpServerDomainName n'est pas réglé, le portail CNP DOIT encore fournir le service d'arbitrage de serveur DNS aux dispositifs IP de réseau LAN.

10 Qualité de service

10.1 Introduction

Le présent paragraphe décrit le rôle de l'environnement IPCable2Home afin de permettre aux applications d'abonné d'utiliser les ressources de qualité de service IPCablecom et DOCSIS. Ces ressources fournissent un mécanisme de gestion qui donne priorité aux flux de session de données afin de prendre en charge le trafic d'applications en temps réel telles que la voix par Internet, la diffusion audiovisuelle et les jeux vidéo, en réduisant la latence des paquets et les délais de gigue. Les mécanismes de qualité de service IPCablecom et DOCSIS permettent aussi une gestion plus efficace du trafic sur le réseau HFC.

La qualité de service définit les exigences d'élément de services PS qui sont nécessaires afin de permettre aux applications IPCablecom d'établir les différents niveaux de qualité de service à travers le réseau HFC.

10.1.1 Objectifs

Les objectifs de qualité de service sont les suivants:

- permettre aux applications d'abonné d'établir des priorités dans les sessions de transmission de données entre le système CMTS et le dispositif HA au moyen d'une messagerie conforme à IPCablecom;
- faciliter la conception et les essais sur site permettant la fabrication et l'interopérabilité de matériels et de logiciels conformes bien qu'issus de vendeurs multiples.

10.1.2 Hypothèses

Les hypothèses suivantes ont été faites pour la qualité de service dans l'environnement IPCable2Home:

- la qualité de service suppose que ces systèmes J.112 et IPCablecom existent sur le réseau câblé;

- afin d'éviter des problèmes avec les fonctions de conversion NAT dans l'élément de portail CAP, les applications conformes à l'environnement IPCablecom utiliseront l'adressage LAN-Pass comme défini aux § 7 et 8.

10.2 Architecture de qualité de service

L'architecture de qualité de service du câble (qualité CQoS) se compose d'éléments fonctionnels IPCable2Home et de la classe de dispositifs HA. Les développeurs d'équipements de réseau (par exemple de matériels et de logiciels) implémentent un ou plusieurs de ces éléments selon l'ensemble de caractéristiques désirées. Les ensembles minimaux de capacités spécifiés doivent obligatoirement faire partie du domaine de la qualité CQoS. Les éléments de base de la qualité CQoS sont présentés au § 10.2.2.

10.2.1 Directives pour la conception du système

La liste des directives pour la conception du système de qualité de service figure dans le Tableau 10-1.

Tableau 10-1/J.191 – Directives pour la conception du système de qualité de service

Numéro	Directives pour la conception du système de qualité de service
QS 1	Il existera un mécanisme normalisé de signalisation de qualité de service permettant aux produits de passerelle résidentielle (HA) de prendre en charge l'établissement de sessions de service rendues prioritaires à travers le réseau DOCSIS pour les applications multimédia.
QS 2	Les applications multimédia peuvent être imbriquées dans le dispositif de passerelle résidentielle (HA) ou dans un dispositif externe connecté selon une technique de mise en réseau du domicile.
QS 4	La qualité CQoS 1.0 doit toujours prendre en charge les deux configurations de dispositif HA: avec service PS imbriqué et avec service PS autonome.
QS 5	Les applications multimédia peuvent inclure des services IPCablecom (E-MTA/S-MTA).

10.2.2 Description du système de qualité de service

L'architecture de la qualité CQoS se compose des entités suivantes:

- domaine de qualité CQoS;
- fonction de services portail (PS);
- fonction de portail de qualité de service du câble (CQP) IPCable2Home;
- dispositif d'accès HA;
- système CMTS.

Le domaine CQoS définit la sphère d'influence directe de la fonctionnalité de qualité CQoS, qui est étendue au dispositif d'accès HA à partir de la tête du réseau câblé. Le service portail et les éléments de portail CQP sont entièrement à l'intérieur du domaine de qualité CQoS et sont spécifiés. Le domaine de qualité CQoS existe pour fournir des services aux applications conformes à IPCablecom.

L'architecture de référence décrit aussi le dispositif d'accès HA. Voir le § 5.

Le système de terminaison de câblo-modem (CMTS) est situé à la tête du réseau câblé et gère les fonctions DOCSIS de qualité de service.

10.2.2.1 Elément de services PS

L'élément de services PS est un élément logique qui contient des composants de portail d'adressage dans le réseau, de gestion, de sécurité et de qualité de service qui fournissent des fonctions de traduction entre le réseau HFC et le réseau du domicile. Le service portail ne réside que dans les dispositifs HA (voir § 5). Le composant de qualité de service est appelé *portail de qualité de service du câble* (CQP).

10.2.2.1.1 Composant de portail CQP

L'élément de services PS contient un composant de portail de qualité de service du câble (CQP) qui joue le rôle de portail de qualité CQoS pour les applications conformes à l'environnement IPCablecom. Sa fonction primaire est de retransmettre la messagerie de qualité de service entre le système CMTS et les applications IPCablecom.

10.2.2.1.2 Configuration de service PS autonome

La présente Recommandation ne définit pas les exigences de qualité QS entre un PS et un CM, de sorte que les fonctions visant à maintenir les priorités de session de transmission de données et à éviter les conflits dus à un accès asynchrone par de multiples dispositifs ne seront pas spécifiées. Il est recommandé que cette interface possède une grande largeur de bande dédiée (non partagée avec d'autres dispositifs) à la connexion PS-CM afin de minimiser la gigue des paquets QS en raison de conflits entre dispositifs multiples.

10.2.2.2 Domaine CQoS

Le domaine CQoS existe sur une base d'utilisateur résidentiel. Les résidences individuelles sont séparées et ont des domaines CQoS indépendants. L'élément de portail CQP fait la limite du domaine CQoS au sein d'une résidence donnée.

10.2.2.3 Classes de dispositifs physiques et éléments fonctionnels de CQoS

Les dispositifs HA contiennent l'élément logique de services portail et l'élément fonctionnel de portail CQP. Le portail CQP agit comme un pont transparent pour la messagerie de qualité de service des applications IPCablecom (APP). Un exemple des relations entre les éléments fonctionnels de CQoS et la classe de dispositifs HA est présenté à la Figure 10-1.

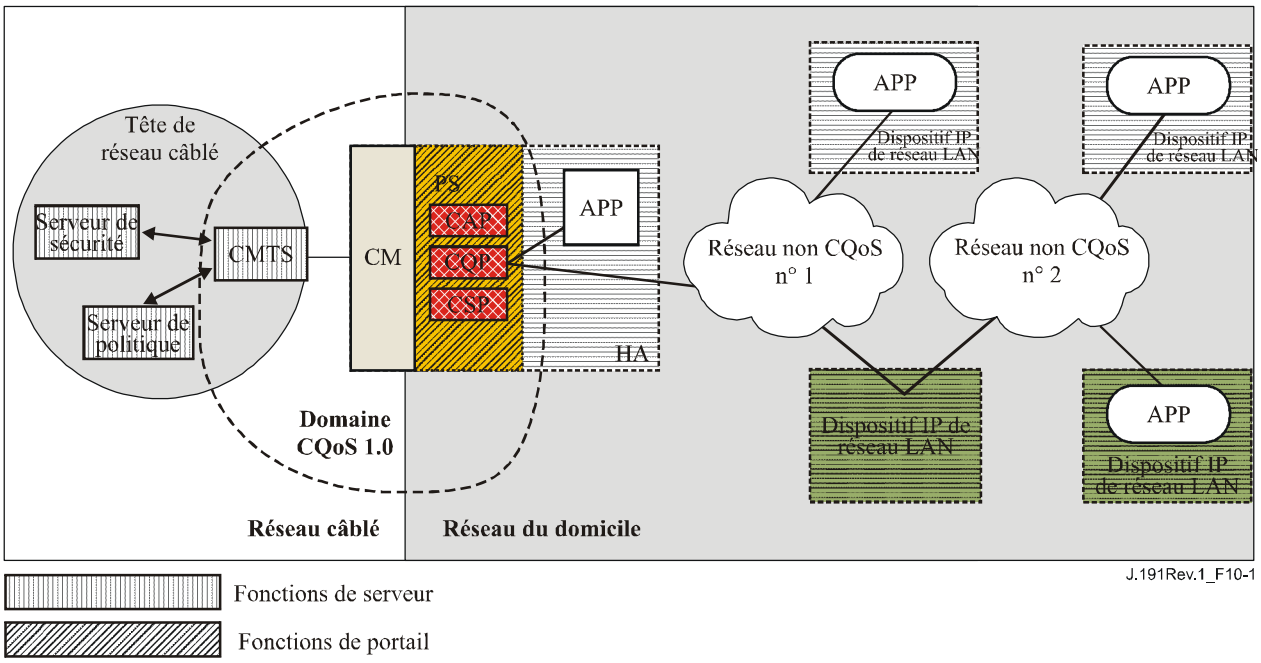


Figure 10-1/J.191 – Exemple d'éléments fonctionnels de qualité CQoS

10.3 Exigences relatives à la messagerie de qualité de service du câble

L'architecture de qualité de service (CQoS) dans l'environnement IPCable2Home se compose de l'élément fonctionnel de portail CQP dans le domaine CQoS. Le portail CQP existe dans le service portail et prend en charge la livraison de la messagerie de qualité de service à travers le réseau HFC pour les applications IPCablecom. La messagerie conforme à IPCablecom inclut la messagerie de qualité de service et d'autres messages en rapport avec les aspects d'un service spécifique comme les décisions de politique et d'application de modèles de réservation à deux phases.

Les exigences fonctionnelles pour le portail CQP et d'autres éléments de CQoS sont définies dans les paragraphes ci-dessous.

10.3.1 Exigences relatives au portail CQP

Le portail CQP DOIT agir comme un pont transparent et transmettre la messagerie de qualité de service IPCablecom (Recommandations UIT-T J.161 et J.163) entre le système CMTS et les applications IPCablecom. Les données d'application sont associées à un flux de service DOCSIS en fonction d'un classificateur qui est créé dans l'interface du câblo-modem sur la base des informations incluses dans les messages IPCablecom (tels que RSVP PATH).

Dans la mesure où les exigences de portail CQP sont simplement de transmettre la messagerie de qualité de service IPCablecom, il n'y a pas de dépendance du système NMS pour assurer cette fonction. Donc, cette fonction CQP reste la même à la fois pour le mode d'approvisionnement DHCP et pour le mode d'approvisionnement SNMP (voir § 5.5).

10.3.2 Gestion de la politique de qualité de service et commande d'admission

La messagerie de qualité de service IPCable2Home est définie par les spécifications IPCablecom (Recommandations UIT-T J.161 et J.163). Comme telles, les fonctions de gestion de la politique de qualité de service et de commande d'admission sont également définies par ces Recommandations IPCablecom.

11 Sécurité

11.1 Introduction/Aperçu général

Le présent paragraphe définit les interfaces de sécurité, les protocoles et les exigences fonctionnelles nécessaires pour fournir fiablement les services IP par câble au dispositif d'accès HA dans un environnement sécurisé.

Assurer la livraison de services IP multimédia aux dispositifs clients chez l'utilisateur exige un mécanisme sécurisé pour protéger ces services des accès illégaux, de l'espionnage et des interruptions. L'objet de toute technologie de sécurité est de protéger la valeur, qu'elle soit un flux de revenu ou un actif d'informations commercialisables d'un certain type. Les menaces contre ce revenu existent lorsqu'un utilisateur du réseau perçoit la valeur, dépense des efforts et de l'argent et invente une technique pour échapper aux payements nécessaires (voir l'Annexe C). Certains utilisateurs du réseau vont très loin pour voler lorsqu'ils perçoivent une valeur extrême. L'ajout de techniques de sécurité afin de protéger la valeur a un coût associé; plus on dépense d'argent, plus grande est la sécurité (l'efficacité de la sécurité relève donc de l'économie de base).

11.1.1 Objectifs

Les objectifs du modèle de sécurité sont les suivants:

- employer une technique de sécurité rentable afin de forcer tout utilisateur ayant l'intention de voler ou d'interrompre des services de réseau à dépenser une quantité déraisonnable de ressources en argent ou en temps;

- sécuriser les connexions résidentielles utilisées pour offrir des services câblés de haute valeur de sorte qu'elles soient au moins aussi sécurisées que les technologies de câblo-modem et IPCablecom sur le réseau hybride optique coaxial (HFC);
- fournir des mécanismes de sécurité flexibles, qui soient compatibles avec les mécanismes de sécurité de câblo-modem et IPCablecom utilisés sur le réseau HFC.

11.1.2 Hypothèses

Les hypothèses relatives à l'environnement de sécurité IPCable2Home sont les suivantes:

- dans le dispositif HA imbriqué (c'est-à-dire dans un PS/CM intégré dans un même dispositif physique), le CM est un câblo-modem J.112 (ou J.122);
- des niveaux de sécurité inférieurs peuvent exister dans le réseau du domicile lorsque les services fournis sont considérés comme étant de basse valeur.

11.2 Architecture de sécurité

L'architecture de sécurité est fondée sur l'architecture générale définie au § 5. L'architecture définit un élément IP de services portail (PS), qui inclut des fonctions de gestion/approvisionnement, sécurité et qualité de service.

L'architecture inclut aussi un ensemble d'éléments de tête de réseau comme le système de terminaison de câblo-modem (CMTS), le serveur de protocole de configuration serveur de dynamique (DHCP), le serveur de gestion de réseau, le serveur de sécurité, etc.

La spécification de sécurité se concentre sur la définition, les fonctionnalités et interfaces des fonctions de sécurité et sur la sécurité qui se rapporte aux serveurs de tête de réseau.

11.2.1 Directives pour la conception du système

La liste des exigences relatives à la conception de la sécurité figure au Tableau 11-1. Cette liste donne des directives pour le développement de la spécification de sécurité.

Tableau 11-1/J.191 – Directives pour la conception du système de sécurité

Référence	Directives pour la conception du système de sécurité
SEC1	L'opérateur aura la capacité de gérer à distance des pare-feu conformes.
SEC2	La conception du système de sécurité comprendra une interface d'enregistrement/ messagerie d'événements de pare-feu permettant à l'opérateur de surveiller et corriger l'activité du pare-feu.
SEC3	Les messages de gestion du pare-feu entre la tête de réseau du câble et le service portail seront authentifiés et facultativement cryptés pour les protéger contre toute surveillance et commandes non autorisées.
SEC4	La conception du système de sécurité comprendra l'authentification mutuelle des éléments.
SEC5	Le niveau de sécurité résidentiel sera tel qu'il ne soit pas facile pour l'abonné moyen d'obtenir un accès illégal au réseau HFC et aux services du câble.
SEC6	Une fois le compte d'un abonné ouvert, l'authentification du service portail avec le système d'approvisionnement de l'opérateur sera automatique.
SEC7	L'opérateur aura la capacité de télécharger vers l'élément de services PS de façon sécurisée des images logicielles, des fichiers de configuration et les règles de pare-feu.
SEC8	La sécurité IPCable2Home apportera à travers le pare-feu la prise en charge nécessaire pour la qualité DQoS sécurisée IPCablecom.
SEC9	Les messages de gestion de réseau entre la tête de réseau et le service portail seront authentifiés et facultativement cryptés afin de les protéger contre toute surveillance et commandes non autorisées.

Le présent paragraphe limite sa portée à ces exigences primaires de sécurité du système, mais tient compte du fait que, dans certains cas, il est souhaitable d'augmenter la sécurité. Les préoccupations d'opérateurs ou de vendeurs individuels peuvent se traduire par des protections de sécurité accrues. La présente Recommandation n'interdit pas l'utilisation de protections supplémentaires, dans la mesure où elles n'entrent pas en conflit avec les intentions et les directives de la présente Recommandation.

11.2.2 Description du système

Le présent paragraphe donne un aperçu général de tous les éléments qui font partie de l'architecture de sécurité.

L'architecture de sécurité inclut les éléments de sécurité suivants:

- domaine de sécurité;
- fonction de services portail (PS);
- fonction de portail de sécurité de câble (CSP);
- pare-feu (FW);
- serveur de sécurité (KDC, centre de distribution de clés).

Le domaine de sécurité définit les frontières de la sphère d'influence directe dans laquelle la fonction de sécurité est étendue au service portail à partir de la tête de réseau. Les éléments de services portail, de portail CSP et de pare-feu sont entièrement à l'intérieur du domaine de sécurité. L'élément de services PS contient des fonctions d'adressage réseau, de portail de gestion et de sécurité. Le portail CSP agit comme l'élément frontière entre le domaine sécurisé et le domaine non sécurisé. Le domaine de sécurité existe afin de fournir des services de sécurité aux dispositifs conformes.

Ces éléments contiennent des fonctionnalités spécifiques du client, du serveur ou du portail et peuvent exister dans différents types de dispositifs physiques. L'architecture définit la classe de dispositif d'accès résidentiel (HA). Un exemple des relations entre les différents éléments de sécurité et les classes de dispositifs HA est présenté à la Figure 11-1, dans laquelle les applications résidentielles sont représentées par l'acronyme *APP* et où le serveur OSS est le serveur du système NMS.

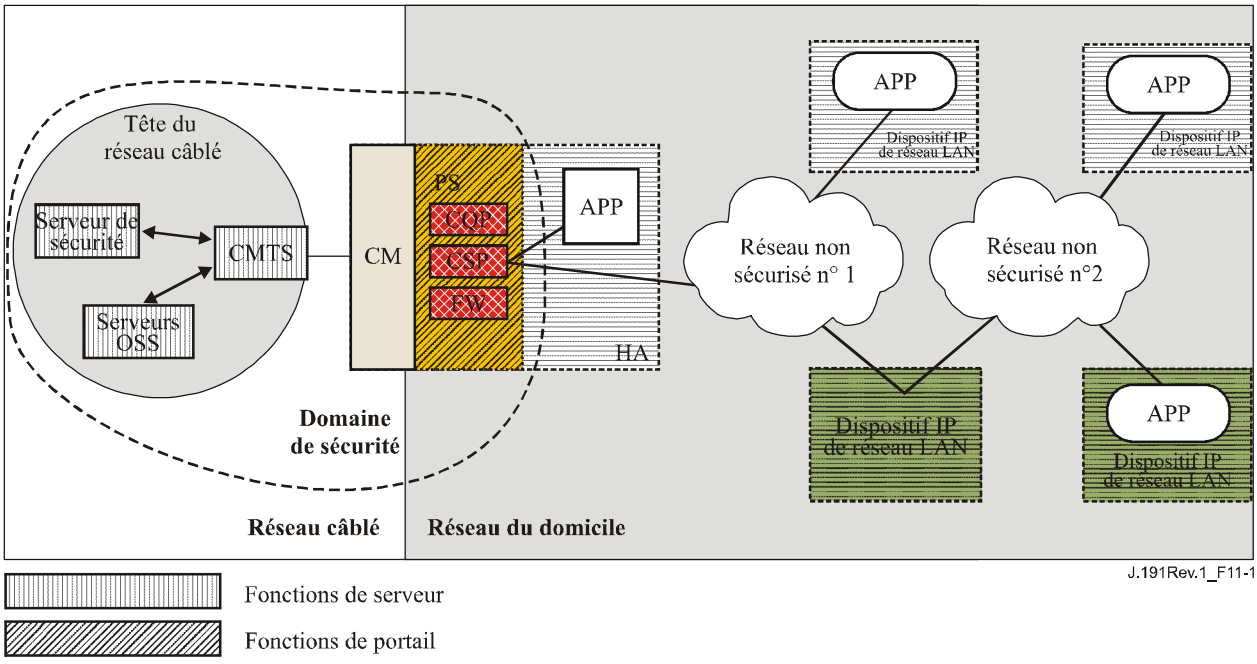


Figure 11-1/J.191 – Eléments de sécurité IPCable2Home

11.2.2.1 Domaine de sécurité

Le domaine de sécurité est défini dans la Figure 11-1. Il englobe l'élément de services PS intégré dans le HA et les serveurs de tête de réseau illustrés.

11.2.2.2 Fonction de services portail

Le service portail (PS) est un élément logique qui contient des fonctions d'adressage réseau, de gestion et de portail de sécurité. Il ne réside que dans les dispositifs HA. Le service portail PS inclut les éléments suivants:

- portail de sécurité de câble (CSP);
- pare-feu (FW).

Le portail CSP agit comme un portail de sécurité pour les autres éléments de services portail. Une de ses fonctions primaires est de transmettre la messagerie de sécurité entre les serveurs OSS de tête de réseau (y compris le serveur de sécurité) et les applications IPCablecom. Le portail CSP fournit aussi des services de sécurité, tels que l'authentification et la gestion de clés, pour l'élément de services PS.

Le service portail inclut aussi une fonction de pare-feu qui assure la protection de l'utilisateur, ainsi que du réseau HFC, contre le trafic indésirable provenant des domaines WAN ou LAN. Un tel trafic peut inclure des attaques délibérées contre le réseau du domicile aussi bien qu'une limitation de trafic pour des applications de contrôle parental.

La spécification de la sécurité ne définira pas en détail la spécification de l'implémentation d'un pare-feu, mais définira à la place un ensemble d'exigences afin de permettre la gestion à distance par l'opérateur.

Typiquement, les pare-feu sont construits à l'aide d'une combinaison de deux composants différents: un filtrage de paquets et un serveur mandataire. Un module de filtrage de paquets est probablement le composant de pare-feu le plus commun parce qu'il détermine quels flux de paquets sont bloqués et quels flux sont autorisés à franchir le pare-feu. Chaque décision individuelle d'abandonner un paquet est fondée sur des informations de configuration statique qui commandent l'inspection des champs d'en-tête de paquet incluant: les adresses IP de source et de destination, les numéros de point d'accès de protocole de source et de destination, le type de protocole, etc. Selon le niveau de sécurité désiré, il peut être nécessaire de configurer un grand nombre de filtres dans un pare-feu, ce qui peut être très difficile et peut requérir une bonne compréhension du type de services (protocoles) à filtrer.

Un mandataire spécifique d'application (ASP), autre composant typique de pare-feu, crée une extrémité et un relais de protocole en implémentant les nécessaires parties client et serveur d'un protocole client-serveur spécifique. La sécurité bénéficie de l'utilisation des mandataires ASP. En premier lieu, il est possible d'ajouter des listes de contrôle d'accès aux protocoles, en exigeant des utilisateurs ou des systèmes qu'ils produisent un certain niveau d'authentification avant de se voir accorder l'accès. Par ailleurs, étant spécifique du protocole, un mandataire ASP comprend le protocole et peut être configuré pour bloquer seulement des sous-parties du protocole. Par exemple, un mandataire ASP du protocole FTP peut être configuré de façon à bloquer le trafic en provenance d'utilisateurs non authentifiés, tandis que les utilisateurs authentifiés se verront attribuer un accès sélectif aux commandes "put" (*mettre*) et "get" (*obtenir*), selon par exemple le sens d'émission de ces commandes.

La combinaison particulière de filtres de paquets et de mandataires ASP dans un pare-feu donné constitue un compromis entre la performance et le niveau de sécurité qu'accorde le pare-feu. Etant typiquement un mécanisme de couche Réseau, les filtres de paquets tendent à donner de meilleures performances que les mandataires ASP, qui sont des mécanismes de couche Application. Une solution de compromis de plus en plus courante consiste à utiliser un filtrage de paquets d'après l'état (SPF, *stateful packet filtering*) où les informations d'état accumulées à partir des paquets

appartenant à la même connexion sont conservées et utilisées dans la prise de décision concernant l'abandon de paquet.

En dernier ressort, les filtrages statiques ou SPF et les mandataires ASP sont les boutons de commande qui servent à implémenter le niveau de sécurité désiré sur un site. Cependant, tandis que la politique de sécurité détermine les services autorisés et la façon dont ils sont utilisés de part et d'autre du pare-feu, la politique de sécurité n'explicite pas la configuration spécifique pour le pare-feu. C'est l'ensemble des règles dérivées de la politique de sécurité qui définit la collection de règles de contrôle d'accès (règles d'action des filtres et mandataires) qui déterminent ensuite quels paquets le pare-feu transmet ou rejette. Calculer l'ensemble de règles des déclarations de la politique de sécurité est un vrai défi car ces dernières sont habituellement exprimées dans un langage humain de haut niveau.

Etant donné qu'un pare-feu n'a besoin que de l'ensemble de règles pour configurer ses composants de filtrage SPF et de mandataire ASP, la définition de la politique de sécurité et la déduction d'un ensemble de règles correspondant sont considérées comme étant en dehors du domaine d'application du pare-feu. Un ensemble de règles approprié doit être configuré dans un pare-feu via un téléchargement de fichier de configuration de pare-feu authentifié. Le format réel du fichier contenant l'ensemble de règles applicables à un pare-feu particulier et la façon dont ce fichier est utilisé dans le pare-feu pour configurer les composants de filtrage SPF et de mandataire ASP est spécifique de l'implémentation. La présente Recommandation ne vise que le mécanisme d'authentification utilisé pour télécharger l'ensemble de règles d'un pare-feu vers l'élément de services PS.

La Figure 11-2 illustre les relations entre les composants du pare-feu. En particulier, la Figure 11-2 suggère qu'un ensemble de règles (RS, *rule set*) doit être utilisé pour la configuration interne des composants du pare-feu. Ces composants sont les fonctions de filtre de paquet entrant (IPF, *inbound packet filter*), de filtre de paquet sortant (OPF, *outbound packet filter*) et de mandataire spécifique d'application (ASP) ou de filtre de paquets d'après l'état (SPF). La Figure 11-2 donne aussi une vue plus détaillée du service portail et de ses relations avec les fonctions de pare-feu et autres composants dans le dispositif d'accès HA. En particulier, la Figure 11-2 suggère que les fonctions de mandataire spécifique de l'application/filtrage de paquets d'après l'état (ASF/SPF) du pare-feu sont intimement associées dans la fonction de traduction d'adresse de couche Réseau (NAT) du portail CAP. Etant donné qu'une fonction de traduction NAT interrompt certaines applications, le traitement spécifique d'application est exigé dans le cadre de l'implémentation de la traduction NAT et l'implémentation du service portail PEUT donc combiner les fonctions ASP/SPF et NAT.

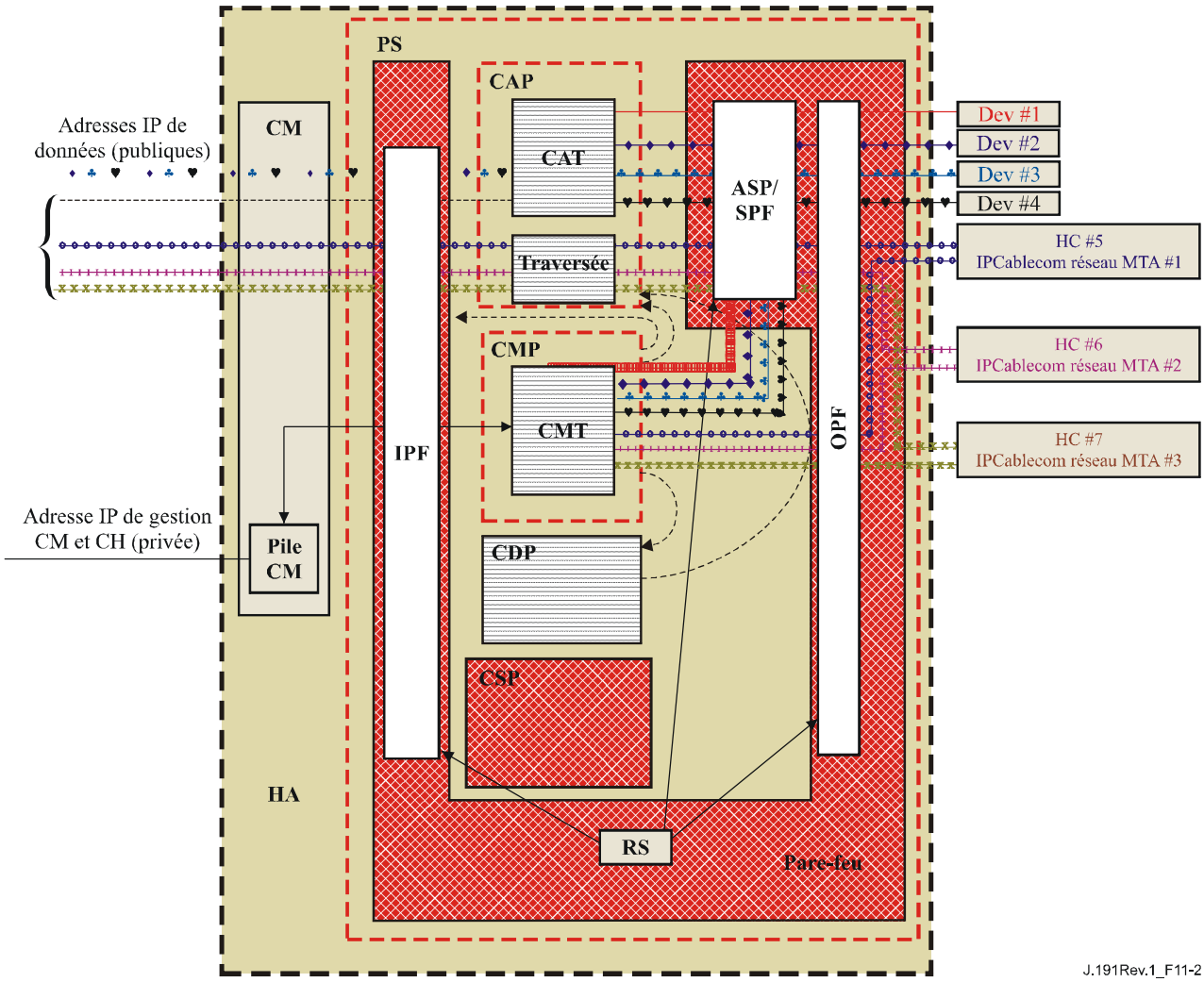


Figure 11-2/J.191 – Exemple d'élément de services PS dans un dispositif d'accès HA

11.2.3 Serveur de centre de distribution de clé (KDC)

Le serveur de sécurité qui est pris en charge dans l'environnement IPCable2Home est le serveur de centre de distribution de clé (KDC, *key distribution centre*). Si un serveur KDC prenant en charge l'environnement IPCable2Home est disponible à la tête de réseau, ce serveur sera utilisé pour assurer les services d'authentification et de distribution de clés au moyen du protocole Kerberos. S'il est disponible, le centre KDC communiquera avec la fonction de portail CSP afin d'établir ces services.

11.2.4 Autres éléments et fonctions associés

Les éléments suivants ne sont pas considérés comme éléments de sécurité mais utilisent effectivement ou prennent part à la gestion de ces services de sécurité.

- système OSS;
- portail CMP.

Le système OSS représente un ensemble de serveurs de tête de réseau qui permettent la gestion des éléments dans l'environnement IPCable2Home. Les serveurs du système OSS communiquent avec le portail CMP afin de gérer les fonctions et services de sécurité. La liaison entre le système OSS et le portail CMP est sécurisée au moyen des services d'authentification et de confidentialité définis dans la présente Recommandation.

Le portail CMP est la fonction de gestion au sein du service portail. L'architecture de sécurité fournit l'authentification et d'autres services de sécurité pour ses communications avec les serveurs OSS situés dans la tête de réseau. Le portail CMP permet la gestion des fonctions de services portail, y compris la gestion des services de sécurité.

On trouvera des détails complémentaires sur ces éléments et sur leurs fonctions aux § 12 et 13, ainsi qu'au § 10 sur la qualité de service.

11.3 Exigences

Pour toutes les références à la sécurité IPCablecom, voir la Rec. UIT-T J.170.

11.3.1 Authentification d'élément

Pour les besoins de la sécurité, il est important de savoir avec qui l'on est en communication avant d'échanger des informations significatives. L'authentification fournit un moyen d'identifier de façon sûre des parties qui ne se connaissent pas et qui veulent communiquer. Il y a trois parties dans l'identification: les pièces justificatives de l'identité, la vérification de la validité des pièces justificatives d'identité et les moyens communs de communiquer les informations d'identité. La présente Recommandation spécifie une pièce justificative d'identification normalisée pour l'industrie, l'utilisation de certificats X.509 en conjonction avec le document RFC 3280. Le certificat d'élément de services PS fournit l'identité de l'élément de services PS associé en liant cryptographiquement l'adresse de commande MAC de l'élément de services PS au certificat de clé publique produit pour cet élément de services PS. De plus, les certificats de clé publique fournissent un moyen sécurisé de communiquer les informations d'identité.

Lorsqu'un centre KDC qui accepte la présente Recommandation est disponible dans la tête de réseau, l'authentification est acceptée. Si un centre KDC est disponible, il est recommandé que le câblo-opérateur fournisse l'élément de services PS en mode d'approvisionnement SNMP (comme décrit au § 5.5) afin de tirer parti du protocole d'authentification mutuelle spécifié en se servant de Kerberos avec l'extension PKINIT. Kerberos offre un protocole permettant une authentification mutuelle sécurisée afin de fournir les matériaux de clé et n'établir les communications qu'entre les parties authentifiées dans le réseau IPCable2Home. Comme ce modèle d'authentification a déjà été spécifié par un autre projet de l'UIT, c'est-à-dire IPCablecom, la présente Recommandation se réfère en tant que de besoin au modèle IPCablecom.

11.3.1.1 Kerberos/PKINIT

Lorsque l'élément de services PS est approvisionné en mode SNMP, la présente Recommandation spécifie l'utilisation de Kerberos avec l'extension de clé publique PKINIT afin d'authentifier les éléments et de prendre en charge les exigences de gestion de clé. Les éléments (les clients) s'authentifient eux-même auprès du centre KDC avec le protocole PKINIT. Une fois authentifiés auprès du centre KDC, les clients peuvent recevoir un ticket Kerberos afin de s'identifier eux-mêmes auprès d'un serveur particulier.

En mode d'approvisionnement SNMP, l'élément de services PS, le système NMS (c'est-à-dire le gestionnaire SNMP) et le centre KDC DOIVENT suivre la spécification relative à Kerberos/PKINIT comme défini dans les § 6.4 et 6.5 de la Rec. UIT-T J.170, sauf indication contraire dans la présente Recommandation. Le centre KDC est équivalent ou identique au centre KDC d'opérateur de systèmes multiples (MSO) dans le modèle IPCablecom (qui spécifie l'utilisation de plusieurs centres KDC). La spécification IPCable2Home utilise le terme de *système de gestion de réseau (NMS)* afin d'offrir cette fonctionnalité SNMP. Dans les références à la suite de spécifications IPCablecom, il est noté que ce système utilise le terme de *serveur d'approvisionnement* afin de désigner la fonctionnalité SNMP. Il y a lieu que le lecteur ne perde pas de vue le fait que cette fonctionnalité SNMP devrait généralement être compatible avec les deux spécifications, bien qu'elles ne soient pas identiques lorsqu'on spécifie des informations spécifiquement IPCablecom et spécifiquement IPCable2Home. L'élément de services PS DOIT agir

comme le client auprès du centre KDC. Dans la Recommandation sur la sécurité IPCablecom, c'est l'adaptateur MTA qui est le client. On suppose que les implémentations IPCable2Home vont utiliser, pour l'élément de services PS, la fonctionnalité client qui est spécifiée pour l'adaptateur MTA. L'élément de services PS utilise Kerberos pour le protocole SNMP. Les certificats utilisés dans le protocole PKINIT sont spécifiés dans le paragraphe de la présente Recommandation qui concerne l'infrastructure de clé publique (PKI). Lorsque le système IPCablecom spécifie un certificat de dispositif adaptateur MTA, la présente Recommandation fournit un certificat pour l'élément de services PS (certificat d'élément de services PS) et les implémentations des éléments de services portail DOIVENT inclure ce certificat d'élément de services PS.

Les paragraphes suivants de la Rec. UIT-T J.170, concernant la fonctionnalité Kerberos, ne sont pas applicables à la présente Recommandation:

- § 6.4.8.4, Préauthentificateur pour la localisation du serveur d'approvisionnement;
- § 6.4.7, Noms des mandants d'adaptateur MTA;
- § 6.4.8, Mappage d'adresse MAC d'adaptateur MTA sur un nom FQDN d'adaptateur MTA;
- § 6.4.10, Suivi des versions des clés de service;
- § 6.4.11, Opération transectorielle Kerberos;
- § 6.5.4, Messages de renouvellement de clé;
- § 6.5.6, Protocole IPsec kerbérisé;
- § 6.4.6, Conventions relatives aux emplacements et aux noms des serveurs Kerberos.

11.3.1.2 Variables d'authentification spécifiquement IPCable2Home

Le modèle IPCablecom spécifie pour Kerberos certains noms de variables spécifiques dans l'architecture de réseau IPCablecom. Afin que la présente Recommandation utilise le modèle IPCablecom, les noms de variables suivants doivent être changés:

- remplacer pktcKdcToMtaMaxClockSkew comme défini dans la spécification IPCablecom de sécurité par KdcToClientMaxClockSkew;
- remplacer pktcSrvrToMtaMaxClockSkew comme défini dans la spécification IPCablecom de sécurité par SrvrToClientMaxClockSkew;
- remplacer mtaprovsrvr tel que défini dans la spécification IPCablecom de sécurité par provsrvr.

Les implémentations Kerberos du modèle IPCable2Home DOIVENT ignorer la portion de champ contenant l'identificateur d'objet (OID), qui se lit clabProjIPCablecom(2) dans les données AppSpecificTypedData des messages KRB-ERROR.

11.3.1.3 Profil IPCable2Home pour les conventions relatives aux emplacements et aux noms des serveurs Kerberos

Dans le secteur Kerberos, les noms PEUVENT utiliser la même syntaxe qu'un nom de domaine mais les secteurs Kerberos DOIVENT être écrits en lettres majuscules. Les détails relatifs au secteur Kerberos DOIVENT être suivis conformément à l'Annexe B/J.170.

Les conventions relatives aux centres KDC, énumérées dans le § 6.4.6.2/J.170, sont considérées comme informatives pour la présente Recommandation avec la réserve que le centre KDC appliquera les fonctions nécessaires sur le plan administratif afin d'échanger les informations appropriées avec le système NMS (serveur d'approvisionnement ou gestionnaire SNMP). L'élément de services PS a fourni au centre KDC, dans le message de demande AS, l'adresse IP du serveur d'approvisionnement en tant qu'information nécessaire pour établir le contact approprié entre le centre KDC et le serveur d'approvisionnement.

Le nom d'un mandant d'élément de services PS DOIT être du type NT-SRV-INST avec exactement deux composants, dont le premier DOIT être la chaîne "PSElement" (sans les guillemets) et dont le second DOIT être l'adresse MAC du réseau WAN-Man, soit:

PSElement/<adresse MAC de WAN-Man>

où l'expression <WAN-Man-MAC> est l'adresse MAC de gestion de réseau WAN de l'élément de services PS. Le format de l'adresse <WAN-Man-MAC> DOIT être: "XX:XX:XX:XX:XX:XX" (sans les guillemets) où X est un caractère hexadécimal de l'adresse de commande MAC. Les caractères hexadécimaux de a à f DOIVENT être écrits en minuscules.

Le nom d'un mandant d'élément de système NMS DOIT être du type NT-SRV-HST avec exactement deux composants, dont le premier DOIT être la chaîne "provsrvr" (sans les guillemets) et dont le second DOIT être l'adresse de l'entité SNMP du fournisseur de services, soit:

provsrvr/<adresse de l'entité SNMP>

où l'expression <adresse de l'entité SNMP> est l'adresse IP de l'entité SNMP du fournisseur de services (sous-option 3 de l'option DHCP 177 d'un client CDC) écrite en notation à points entre crochets (p. ex. [12.34.56.78]).

11.3.2 Infrastructure de clé publique (PKI)

La présente Recommandation utilise des certificats de clé publique conformes à la Rec. UIT-T X.509 | ISO/CEI 9594-8 et au document RFC 3280 du groupe IETF.

11.3.2.1 Structure générique

11.3.2.1.1 Version

La version des certificats DOIT être Rec. UIT-T X.509 v3, ce qui est noté comme v2 dans le certificat final (parce que la version v1 n'a pas eu de numéro de version associé). Tous les certificats DOIVENT être conformes au document RFC 3280 excepté lorsque la non-conformité avec le document RFC est explicitement déclarée dans le présent paragraphe. Toute demande de non-conformité selon la présente Recommandation quant au contenu n'implique pas la non-conformité quant au format. Toute demande spécifique de non-conformité quant au format sera décrite explicitement.

11.3.2.1.2 Type de clé publique

Les clés publiques à codage RSA sont utilisées dans toute la hiérarchie des certificats décrite au § 11.3.2.2. L'identificateur d'objet subjectPublicKeyInfo.algorithm utilisé DOIT être à la valeur 1.2.840.113549.1.1.1 (rsaEncryption).

L'exposant public pour toutes les clés RSA DOIT être F_4 – 65537.

11.3.2.1.3 Extensions

Les extensions (subjectKeyIdentifier, authorityKeyIdentifier, KeyUsage et BasicConstraints) DOIVENT suivre le document RFC 3280. Toute autre extension de certificat PEUT aussi être incluse car non critique. Les balises de codage sont [c:critique, n:non critique; m:obligatoire, o:facultatif] et sont identifiées dans le tableau relatif à chaque certificat.

11.3.2.1.3.1 subjectKeyIdentifier

L'extension subjectKeyIdentifier incluse dans tous les certificats comme l'exige le document RFC 3280 (par exemple, tous les certificats excepté les certificats de dispositif et d'auxiliaires) DOIT inclure la valeur keyIdentifier composée du hachage SHA-1 sur 160 bits de la valeur de la chaîne binaire (BITSTRING) subjectPublicKey (excluant la balise, la longueur et le nombre de bits inutilisés du codage ASN.1) (voir le document RFC 3280).

11.3.2.1.3.2 Extension authorityKeyIdentifier

L'extension authorityKeyIdentifier, incluse dans tous les certificats comme l'exige le document RFC 3280, DOIT inclure l'identificateur subjectKeyIdentifier tiré du certificat de l'émetteur (voir le document RFC 3280) à l'exception des certificats radicaux.

11.3.2.1.3.3 Extension KeyUsage

L'extension keyUsage DOIT être utilisée pour tous les certificats d'autorité de certification (CA, *certificate authority*) et pour tous les certificats de vérification de code (CVC). Pour les certificats d'autorité CA, l'extension keyUsage DOIT être marquée comme critique avec une valeur de keyCertSign et cRLSign. Pour les certificats de code CVC, l'extension keyUsage DOIT être marquée comme critique avec une valeur de digitalSignature et keyEncipherment. Les certificats d'entité de terminaison peuvent utiliser l'extension keyUsage comme indiqué dans RFC 3280.

11.3.2.1.3.4 Extension BasicConstraints

L'extension basicConstraints DOIT être utilisée pour tous les certificats d'autorité CA et de code CVC et DOIT être marquée comme critique. Les valeurs propres à chaque certificat pour basicConstraints DOIVENT être marquées comme spécifié dans les Tableaux 11-2 à 11-13 de description de certificat.

11.3.2.1.4 Algorithme de signature

Le mécanisme de signature utilisé DOIT être SHA-1 [FIPS 186-2] avec codage RSA. L'identificateur OID spécifique est 1.2.840.113549.1.1.5.

11.3.2.1.5 Chaînes SubjectName et IssuerName

Si une chaîne ne peut pas être codée comme une chaîne PrintableString, elle DOIT être codée comme une chaîne UTF8String (balise [UNIVERSAL 12]).

Lors du codage d'un nom X.500:

- chaque nom distinctif relatif (RDN) DOIT contenir un seul élément de l'ensemble des attributs X.500;
- l'ordre des noms RDN dans un nom X.500 DOIT être le même que l'ordre dans lequel ils sont présentés dans la présente Recommandation.

11.3.2.1.6 Numéro de série

Le numéro de série DOIT être un nombre entier, positif et unique, attribué par l'autorité CA à chaque certificat (c'est-à-dire que le nom de l'émetteur et le numéro de série désignent un certificat unique). Les autorités CA DOIVENT forcer le numéro de série à être un entier non négatif. Le constructeur NE DEVRAIT PAS imposer ou suggérer de relation entre le numéro de série du certificat et celui du modem auquel le certificat est envoyé.

Compte tenu des exigences d'unicité ci-dessus, l'on peut prévoir que les numéros de série contiendront des entiers longs. Les utilisateurs des certificats DOIVENT être en mesure de prendre en charge des valeurs de numéro de série pouvant atteindre 20 octets.

11.3.2.2 Hiérarchies des certificats IPCable2Home

Trois hiérarchies de certificat distinctes sont utilisées. La chaîne de constructeur sert à identifier les constructeurs autorisés; la chaîne de code de vérification sert à identifier les images logicielles conformes; la chaîne de fournisseur de services sert à identifier les dispositifs contenus dans le réseau du fournisseur de services pour l'authentification mutuelle avec les dispositifs de l'abonné.

Les hiérarchies de certificat décrites dans la présente Recommandation peuvent s'appliquer à tous les projets de l'UIT qui ont besoin de certificats. Chaque projet peut adopter cette hiérarchie car il est possible de migrer vers une structure de certificat partagée et plus générique. De même, chaque

projet peut avoir besoin d'apporter aux exigences des ajustements spécifiques pour ce projet particulier. L'objectif est de créer une infrastructure PKI qui puisse être réutilisée pour chaque projet. Il peut y avoir des différences entre les certificats d'entité terminale exigés pour chaque projet mais, lorsque les certificats d'entité terminale se recouvrent, un même certificat d'entité terminale pourrait être utilisé pour plusieurs services dans la même infrastructure câblée. Par exemple, le modèle IPCablecom exige un centre KDC pour le fournisseur de services et le modèle IPCable2Home exige également un centre KDC pour le fournisseur de services. Si celui-ci fait tourner les deux architectures de réseau sur ses systèmes, il peut utiliser le même centre KDC et le même certificat de centre KDC pour les communications dans les deux systèmes, c'est-à-dire IPCablecom et IPCable2Home. Dans ce cas, le centre KDC du modèle IPCable2Home est équivalent ou identique au centre KDC de l'opérateur MSO du modèle IPCablecom (qui spécifie l'utilisation de plusieurs centres KDC).

Dans la Figure 11-3 ci-dessous, le terme "autorité de certification" est abrégé en CA et le terme "certificat de vérification de code" est abrégé en CVC.

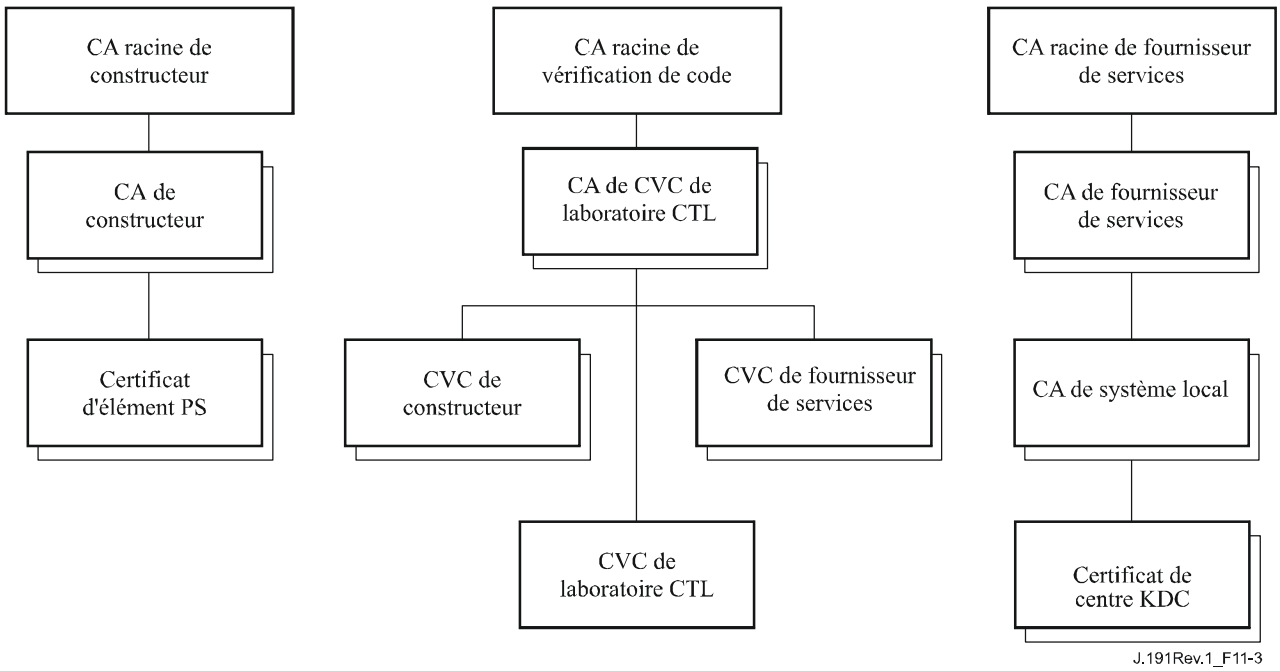


Figure 11-3/J.191 – Hiérarchie des certificats IPCable2Home

11.3.2.2.1 Hiérarchie des certificats de constructeur

La hiérarchie des certificats de constructeur ou de chaîne de constructeurs est enracinée dans une autorité racine de constructeur qui sert à émettre des certificats d'autorité de certification (CA) de constructeur pour un ensemble de constructeurs autorisés. Ceux-ci utilisent leur autorité CA pour émettre des certificats individuels d'élément de services PS. Cette chaîne sert à l'authentification des dispositifs résidentiels.

Les informations contenues dans les tableaux ci-après sont les valeurs spécifiques pour les champs exigés conformément au document RFC 3280. Ces valeurs spécifiques de la hiérarchie de certificat de constructeur DOIVENT être suivies conformément aux Tableaux 11-2, 11-3 et 11-4. Si un champ exigé n'est pas spécifiquement inscrit dans les tableaux, les directives du document RFC 3280 DOIVENT alors être suivies. Les extensions génériques DOIVENT aussi être incluses comme spécifié au § 11.3.2 (infrastructure PKI).

11.3.2.2.1.1 Certificat CA racine de constructeur

Le certificat CA racine de constructeur (voir Tableau 11-2) DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA racine de constructeur, le certificat CA de constructeur et le certificat d'élément de services PS.

Tableau 11-2/J.191 – Certificat CA racine de constructeur

Forme du nom du titulaire	C=<pays> O= CN=autorité CA racine du constructeur
Usage prévu	Ce certificat sert à émettre des certificats CA de constructeur.
Signé par	Autosigné
Période de validité	20 ans au moins
Module de longueur	2048
Extensions	KeyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], basicConstraints [c,m](cA=true).

11.3.2.2.1.2 Certificat CA de constructeur

Le certificat CA de constructeur DOIT être vérifié en tant que partie d'une chaîne de certificats contenant le certificat CA racine du constructeur, le certificat CA du constructeur et le certificat d'élément de services PS.

Le pays/la région, la ville et l'usine du constructeur sont des attributs facultatifs. Un constructeur PEUT avoir plus d'un certificat CA de constructeur. Si un constructeur utilise plus d'un certificat CA de constructeur, l'élément de services PS DOIT avoir accès au certificat approprié tel que vérifié en faisant correspondre le nom de l'émetteur contenu dans le certificat d'élément de services PS avec le nom du titulaire contenu dans le certificat CA du constructeur. S'il est présent, l'identificateur authorityKeyIdentifier du certificat d'élément de services PS DOIT être mis en correspondance avec l'identificateur subjectKeyIdentifier du certificat du constructeur, comme décrit dans RFC 3280.

Tableau 11-3/J.191 – Certificat CA d'un constructeur

Forme du nom de titulaire	C=<pays> O=<nom de l'entreprise> [ST=<état/région>] [L=<ville>] OU= [OU=<usine du constructeur>] CN=<nom de l'entreprise> Mfg CA
Usage prévu	Ce certificat est émis pour chaque constructeur par l'autorité CA racine du constructeur et peut être fourni à chaque élément de services PS soit au moment de la fabrication, soit pendant une mise à jour de code de champ. Ce certificat apparaît comme un paramètre en lecture seule dans la base MIB d'élément de services PS. Ce certificat produit des certificats d'élément de services PS. Ce certificat, avec le certificat CA racine de constructeur et le certificat d'élément de services PS, sert à authentifier l'identité de l'élément de services PS. La liste optionnelle des installations du fabricant peut être constituée du nom des installations et/ou de leur lieu d'implantation.

Tableau 11-3/J.191 – Certificat CA d'un constructeur

Signé par	L'autorité CA racine du constructeur
Période de validité	20 ans
Longueur du module	2048
Extensions	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m] basicConstraints[c,m](cA=true, pathLenConstraint=0)

Le nom de l'entreprise inséré dans le champ d'organisation (O) PEUT être différent du nom d'entreprise (CN) inséré dans le champ de nom courant.

11.3.2.2.1.3 Certificat d'élément de services PS

Le certificat d'élément de services PS DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA racine de constructeur, le certificat CA de constructeur et le certificat d'élément de services PS.

Le pays/la région, la ville, le nom du produit et l'usine du constructeur sont des attributs facultatifs.

L'adresse de commande MAC de réseau WAN-Man de l'élément de services PS DOIT être exprimée par six paires de chiffres hexadécimaux séparés par deux points, par exemple "00:60:21:A5:0A:23". Les caractères hexadécimaux alphabétiques (A à F) DOIVENT être exprimés en majuscules.

Un certificat d'élément de services PS est installé de façon permanente, non renouvelable et non remplaçable. Donc, le certificat d'élément de services PS DOIT avoir une période de validité plus grande que la durée de vie de fonctionnement attendue du dispositif spécifique.

Tableau 11-4/J.191 – Certificat d'élément de services PS

Forme du nom de titulaire	C=<pays> O=<nom de l'entreprise> [ST=<état/région>] [L=<ville>] OU=IPCable2Home [OU=<nom de produit>] [OU=<usine du constructeur>] CN=<adresse de commande MAC du réseau WAN-Man>
Usage prévu	Ce certificat est émis par l'autorité CA du constructeur et installé en usine. Le serveur du système NMS ne peut pas mettre à jour ce certificat. Ce certificat apparaît comme un paramètre en lecture seule dans la base MIB d'élément de services PS. Ce certificat sert à authentifier l'identité de l'élément de services PS.
Signé par	Autorité CA du constructeur
Période de validité	20 ans au moins
Longueur du module	1024, 1536, 2048
Extensions	keyUsage[c,m](digitalSignature, keyEncipherment), authorityKeyIdentifier [n,m].

11.3.2.2.2 Hiérarchie de certificat de vérification de code

La hiérarchie de certificat de vérification de code (CVC), ou chaîne de vérification de code s'enracine dans une autorité CA racine de vérification de code, qui émet le certificat CA de vérification de code. L'autorité CA de vérification de code sert à émettre des certificats CVC pour un ensemble de constructeurs et de fournisseurs de services autorisés. L'autorité CA de vérification de code produit aussi les certificats CVC. Cette chaîne sert spécifiquement à authentifier les téléchargements de logiciels. L'infrastructure PKI permet des certificats CVC de constructeur, un certificat CVC et des certificats CVC de fournisseur de services.

Les informations contenues dans les tableaux ci-après sont les valeurs spécifiques pour les champs exigés, conformément au document RFC 3280. Ces valeurs spécifiques pour la hiérarchie de certificat de vérification de code DOIVENT être suivies conformément aux Tableaux 11-5, 11-6, 11-7, 11-8 et 11-9 ci-dessous. Si un champ exigé ne figure pas spécifiquement dans ces tableaux, on DOIT alors suivre les directives du document RFC 3280. Les extensions génériques DOIVENT être aussi incluses comme spécifié au § 11.3.2 (Infrastructure PKI).

11.3.2.2.2.1 Certificat CA racine de vérification de code

Ce certificat DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA de vérification de code, l'autorité CA de vérification de code et les certificats de vérification de code.

Tableau 11-5/J.191 – Certificat CA racine de vérification de code

Forme du nom de titulaire	C=<pays> O= CN=autorité CA racine de certificat CVC
Usage prévu	Ce certificat sert à signer les certificats CA de vérification de code
Signé par	Autosigné
Période de validité	20 ans au moins
Longueur du module	2048
Extensions	KeyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], basicConstraints [c,m](cA=true).

11.3.2.2.2.2 Certificat CA de vérification de code

Le certificat CA de vérification de code DOIT être vérifié en tant que partie d'une chaîne de certificats contenant le certificat CA racine de vérification de code, le certificat CA de vérification de code et le certificat de vérification de code. Un service PS autonome ne DOIT prendre en charge qu'une seule autorité CA de vérification de code à la fois.

Tableau 11-6/J.191 – Certificat CA de vérification de code

Forme du nom de titulaire	C=<pays> O= CN=autorité CA de certificat CVC
Usage prévu	Ce certificat est produit par l'autorité CA racine de vérification de code. Ce certificat produit les certificats de vérification de code.
Signé par	Autorité CA racine de vérification de code
Période de validité	20 ans

Tableau 11-6/J.191 – Certificat CA de vérification de code

Longueur du module	2048
Extensions	KeyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints [c,m](cA=true, pathLenConstraint=0).

11.3.2.2.2.3 Certificat de vérification de code constructeur

Ce certificat DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA racine de vérification de code, le certificat CA de vérification de code et les certificats de vérification de code.

Tableau 11-7/J.191 – Certificat de vérification de code de constructeur

Forme du nom de titulaire	C=<pays> O=<nom de l'entreprise> [ST=<état/région>] [L=<ville>] CN=<nom de l'entreprise> Mfg CVC
Usage prévu	L'autorité CA de vérification de code produit ce certificat pour chaque constructeur autorisé. Il sert à la politique établie par le câblo-opérateur pour le téléchargement de logiciel sécurisé. Le nom d'entreprise peut être différent dans les champs O et CN.
Signé par	Autorité CA de vérification de code
Période de validité	10 ans au plus
Longueur du module	1024, 1536, 2048
Extensions	keyUsage[c,m](digitalSignature, keyEncipherment), extendedKeyUsage [c,m] (id-kp-codeSigning), authorityKeyIdentifier [n,m].

11.3.2.2.2.4 Certificat de vérification de code

Le certificat de vérification de code DOIT être vérifié en tant que partie d'une chaîne de certificats contenant le certificat CA racine de vérification de code, le certificat CA de vérification de code et le certificat de vérification de code.

Tableau 11-8/J.191 – Certificat de vérification de code

Forme du nom de titulaire	C=<pays> O= CN=certificat CVC
Usage prévu	L'autorité CA de vérification de code produit ce certificat, qui sert à authentifier le code certifié. Il est utilisé dans la politique établie par le câblo-opérateur pour le téléchargement de logiciel sécurisé.
Signé par	Autorité CA de vérification de code
Période de validité	10 ans au plus

Tableau 11-8/J.191 – Certificat de vérification de code

Longueur du module	1024, 1536, 2048
Extensions	keyUsage[c,m](digitalSignature, keyEncipherment), extendedKeyUsage [c,m] (id-kp-codeSigning), authorityKeyIdentifier [n,m].

11.3.2.2.2.5 Certificat de vérification de code de fournisseur de services

Le certificat de vérification de code de fournisseur de services DOIT être vérifié en tant que partie d'une chaîne de certificats contenant le certificat CA racine de vérification de code, le certificat CA de vérification de code et le certificat de vérification de code de fournisseur de services.

Tableau 11-9/J.191 – Certificat de vérification de code de fournisseur de services

Forme du nom de titulaire	C=<pays> O=<nom de l'entreprise> [ST=<état/région>] [L=<ville>] CN=<nom de l'entreprise> Certificat CVC de fournisseur de services
Usage prévu	L'autorité CA de vérification de code produit ce certificat pour chaque fournisseur de services autorisé. Il sert à la politique établie par le câblo-opérateur pour le téléchargement de logiciel sécurisé. Le nom d'entreprise peut être différent dans les champs O et CN.
Signé par	Autorité CA racine de vérification de code
Période de validité	10 ans au plus
Longueur du module	1024, 1536, 2048
Extensions	keyUsage[c,m](digitalSignature, keyEncipherment), extendedKeyUsage [c,m] (id-kp-codeSigning), authorityKeyIdentifier [n,m]

11.3.2.2.3 Hiérarchie de certificat de fournisseur de services

La hiérarchie de certificat de fournisseur de services, ou chaîne de fournisseur de services, s'enracine dans l'autorité CA racine de fournisseur de services qui est utilisée pour émettre des certificats pour un ensemble de fournisseurs de service autorisés. L'autorité CA de fournisseur de services peut être utilisée pour émettre des certificats facultatifs de système local ou des certificats auxiliaires. Si l'autorité CA de fournisseur de services ne produit pas les certificats auxiliaires, cela sera alors fait par l'autorité CA de système local. Les certificats auxiliaires sont les certificats d'entité terminale sur le réseau du câblo-opérateur.

Les informations contenues dans les tableaux suivants sont les valeurs spécifiques pour les champs exigés, conformément au document RFC 3280. Ces valeurs spécifiques pour la hiérarchie de certificat de fournisseur de services DOIVENT être suivies conformément aux Tableaux 11-10 à 11-13 ci-dessous. Si un champ exigé ne figure pas spécifiquement dans ces tableaux, les directives du document RFC 3280 DOIVENT alors être suivies. Les extensions génériques DOIVENT aussi être incluses comme spécifié au § 11.3.2 (infrastructure PKI).

11.3.2.2.3.1 Certificat CA racine de fournisseur de services

Ce certificat DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA racine de fournisseur de services, le certificat CA de fournisseur de services, le certificat facultatif de système local et les certificats auxiliaires.

Tableau 11-10/J.191 – Certificat CA racine de fournisseur de services

Forme du nom de titulaire	C=<pays> O= CN=autorité CA racine de fournisseur de services
Usage prévu	Ce certificat est utilisé pour produire les certificats CA de fournisseur de services.
Signé par	Autosigné
Période de validité	20 ans au moins.
Longueur du module	2048
Extensions	KeyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], basicConstraints [c,m](cA=true)

11.3.2.2.3.2 Certificat CA de fournisseur de services

Le certificat CA de fournisseur de services DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA racine de fournisseur de services, le certificat CA de fournisseur de services, le certificat facultatif de système local et les certificats auxiliaires.

Tableau 11-11/J.191 – Certificat CA de fournisseur de services

Forme du nom de titulaire	C=<pays> O=<nom de l'entreprise> CN=<nom de l'entreprise> Autorité CA de fournisseur de services
Usage prévu	L'autorité CA racine de fournisseur de services produit ce certificat pour chaque fournisseur de services. Afin de faciliter la mise à jour de ce certificat, chaque élément de réseau est configuré avec l'attribut OrganizationName du nom SubjectName du certificat CA de fournisseur de services. C'est le seul attribut qui doit rester constant dans le certificat. Ce certificat apparaît comme un paramètre en lecture seule dans l'objet de base MIB qui identifie l'attribut OrganizationName pour le secteur Kerberos. L'élément n'accepte pas les certificats de fournisseur de services qui ne correspondent pas à cette valeur de l'attribut OrganizationName dans le nom SubjectName. Si la tête de réseau contient un centre KDC qui accepte cette application, l'élément de services PS doit alors effectuer le premier échange PKINIT avec le centre KDC juste après un réamorçage, moment auquel les tableaux de la base MIB ne sont pas encore configurés. A ce moment, le client Kerberos DOIT accepter tout attribut OrganizationalName de fournisseur de services, mais DOIT ultérieurement vérifier que la valeur ajoutée dans la base MIB pour ce secteur est le même que celle qui est contenue dans la réponse PKINIT initiale. Cette autorité CA produit les certificats CA de système local ou les certificats auxiliaires.
Signé par	Autorité CA racine de fournisseur de services.

Tableau 11-11/J.191 – Certificat CA de fournisseur de services

Période de validité	20 ans
Longueur du module	2048
Extensions	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints[c,m](cA=true, pathLenConstraint=1)

Le nom d'entreprise inséré dans le champ d'organisation (O) PEUT être différent du nom d'entreprise (CN) inséré dans le champ de nom courant.

11.3.2.2.3.3 Certificat CA de système local

Ce certificat est facultatif pour le fournisseur de services. Si ce certificat existe, il DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA racine de fournisseur de services, le certificat CA de fournisseur de services, le certificat facultatif de système local et les certificats auxiliaires.

Tableau 11-12/J.191 – Certificat CA de système local

Forme du nom de titulaire	C=<pays> O=<nom de l'entreprise> OU=<nom de système local> CN=<nom de l'entreprise> Autorité CA de système local
Usage prévu	Ce certificat est facultatif et, s'il existe, est produit par l'autorité CA de fournisseur de services. Cette autorité CA produit des certificats auxiliaires. Les serveurs de réseau sont autorisés à se déplacer librement entre autorités CA régionales du même fournisseur de services.
Signé par	Autorité CA de fournisseur de services
Période de validité	20 ans
Longueur du module	1024, 1536, 2048
Extensions	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints[c,m](cA=true, pathLenConstraint=0).

Le nom de l'entreprise inséré dans le champ d'organisation (O) PEUT être différent du nom d'entreprise (CN) inséré dans le champ de nom courant.

11.3.2.2.3.4 Certificat de centre KDC

Ce certificat DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA racine de fournisseur de services, le certificat CA de fournisseur de services, le certificat facultatif de système local et les certificats auxiliaires (par exemple, les certificats de centre KDC).

Le certificat de centre KDC DOIT inclure le nom subjectAltName d'authentification PKINIT de Kerberos comme spécifié dans la spécification IPCablecom sur la sécurité dans le § 8.2.4.1/J.170.

Tableau 11-13/J.191 – Certificat de centre KDC

Forme du nom de titulaire	C=<pays> O=<nom de l'entreprise> [OU=<nom de système local>] OU=centre de distribution de clé CN=<nom du serveur DNS>
Usage prévu	Ce certificat est produit soit par l'autorité CA de fournisseur de services soit par l'autorité CA de système local. Il sert à authentifier l'identité du centre KDC auprès des clients Kerberos pendant les échanges d'authentification PKINIT. Ce certificat est transmis à l'élément de services PS dans la réponse PKINIT.
Signé par	Autorité CA de fournisseur de services ou de système local
Période de validité	20 ans
Longueur du module	1024, 1536, 2048
Extensions	keyUsage[c,o](digitalSignature) authorityKeyIdentifier[n,m](keyIdentifier=<subjectKeyIdentifier value from CA certificate>) subjectAltName[n,m] (voir Annexe C/J.170)

11.3.2.3 Validation de certificat

La validation de certificat implique la validation d'une chaîne de certificats liés depuis les certificats d'entité terminale jusqu'à la racine valide. Par exemple, la signature portée sur le certificat d'élément de services PS est vérifiée avec le certificat CA de constructeur et ensuite la signature portée sur le certificat CA de constructeur est vérifiée avec le certificat CA racine de constructeur. Le certificat CA racine de constructeur est autosigné et ce certificat est reçu d'une source autorisée d'une façon sécurisée. La clé publique présente dans le certificat CA racine de constructeur sert à valider la signature portée sur le même certificat.

Les règles exactes pour la validation de la chaîne de certificat DOIVENT se conformer pleinement au document RFC 3280, où elles sont désignées par l'expression "validation de chemin de certificat". En général, les certificats X.509 acceptent un ensemble de règles souples pour déterminer si le nom de l'émetteur d'un certificat correspond au nom de titulaire d'un autre. Les règles sont telles que deux champs de nom peuvent être déclarés en correspondance même si une comparaison binaire des deux champs de nom n'indique pas de correspondance. Le document RFC 3280 recommande que les autorités de certificat interdisent le codage des champs de nom de telle sorte qu'une implémentation puisse déclarer une correspondance ou une non-correspondance en utilisant une simple comparaison binaire. Cette spécification de sécurité suit la présente Recommandation. En conséquence, le champ tbsCertificate.issuer codé en règles DER d'un certificat DOIT être une correspondance exacte du champ tbsCertificate.subject codé en règles DER du certificat de son émetteur. Une implémentation PEUT comparer le nom de l'émetteur avec son nom de titulaire en effectuant une comparaison binaire des champs tbsCertificate.issuer et tbsCertificate.subject codés en règles DER.

La validation des périodes de validité pour l'imbrication n'est pas vérifiée et n'est pas mise en œuvre intentionnellement, ce qui est conforme aux normes en vigueur. Au moment de son émission, la date de début de validité d'un quelconque certificat d'entité terminale DOIT être identique ou postérieure à la date de début de la période de validité du certificat de l'autorité CA qui l'émet. Après le renouvellement d'un certificat d'autorité CA, les dates de début des certificats des entités terminales PEUVENT être antérieures à la date de début du certificat d'autorité CA de production. La date de fin de validité pour les entités peut être antérieure, égale ou postérieure à la date de fin de validité pour l'autorité CA, comme spécifié dans les tableaux de certificats.

11.3.2.3.1 Validation pour la chaîne de constructeur et la vérification de racine

Le centre KDC DOIT valider la chaîne de certificats de constructeur liée. Habituellement, le premier certificat de la chaîne n'est pas explicitement inclus dans la chaîne de certificats qui est envoyée sur le câble. Si le certificat CA racine de constructeur est explicitement inclus dans la transmission, il DOIT déjà être connu du vérificateur avant le moment de cette vérification de certificat. Le certificat CA racine de constructeur transmis NE DOIT contenir aucun changement du certificat à l'exception possible du numéro de série du certificat, de la période de validité et de la valeur de la signature. Si des changements autres que le numéro de série du certificat, sa période de validité et sa valeur de signature existent dans le certificat CA racine de constructeur transmis par rapport au certificat CA racine de constructeur connu, le centre KDC faisant la comparaison DOIT déclarer que la vérification du certificat échoue.

11.3.2.3.2 Validation pour la chaîne de vérification de code et la vérification de racine

Un serveur administratif peut vérifier la validité de la chaîne de vérification de code avant de commencer le processus de téléchargement de logiciel. Pour des précisions, voir le § 11.3.7.

11.3.2.3.3 Validation pour la chaîne de fournisseur de services et la vérification de racine

L'élément de services PS DOIT valider la chaîne de certificats de fournisseur de services liée. Habituellement, le premier certificat de la chaîne n'est pas explicitement inclus dans la chaîne de certificats envoyée sur le câble. Si le certificat CA racine de fournisseur de services est explicitement inclus dans la transmission, il DOIT être déjà connu du vérificateur avant le moment de la vérification de ce certificat. Le certificat CA racine de fournisseur de services NE DOIT contenir aucun changement dans le certificat, à l'exception possible du numéro de série du certificat, de la période de validité et de la valeur de la signature. Si des changements autres que le numéro de série du certificat, sa période de validité et sa valeur de signature existent dans le certificat CA racine de fournisseur de services transmis par rapport au certificat CA racine de fournisseur de services connu, l'élément PS faisant la comparaison DOIT déclarer que la vérification du certificat échoue.

11.3.2.4 Révocation de certificat

La révocation de certificat fera l'objet d'un complément d'étude.

11.3.3 Messagerie de gestion sécurisée

L'algorithme de sécurité utilisé pour initialiser la messagerie de gestion SNMP dépend du mode d'approvisionnement de l'élément de services PS (voir § 5.5). Il y a deux types de mode d'approvisionnement: le mode d'approvisionnement DHCP et le mode d'approvisionnement SNMP. Le mode d'approvisionnement DHCP a des sous-modes supplémentaires qui permettent de savoir s'il est configuré pour le mode NmAccess ou pour le mode de coexistence. Le mode d'approvisionnement SNMP exige la version SNMPv3 pour la messagerie de gestion.

Les paragraphes suivants décrivent les algorithmes et exigences de sécurité nécessaires pour initialiser la messagerie de gestion SNMP fondée sur le mode d'approvisionnement de l'élément de services PS, lequel DOIT accepter les algorithmes de sécurité SNMPv3 spécifiés aux § 11.3.3.1.2 et 11.3.3.2.

11.3.3.1 Algorithmes de sécurité pour SNMP en mode d'approvisionnement DHCP

En mode d'approvisionnement DHCP, l'élément de services PS peut être configuré pour le mode NmAccess ou pour le mode de coexistence. En mode de coexistence, l'élément de services PS peut être configuré pour les versions SNMPv1, SNMPv2 et/ou SNMPv3 de la messagerie de gestion.

11.3.3.1.1 Mode NmAccess

Si l'élément de services PS est fourni en mode d'approvisionnement DHCP avec le mode NmAccess, la gestion de réseau fondée sur SNMP au sein de l'élément de services PS n'utilise pas la version SNMPv3 et n'a donc pas besoin d'initialiser les fonctions de sécurité SNMPv3. L'initialisation de la liaison de gestion SNMPv1/v2 est définie au § 6.3.6.1.

11.3.3.1.2 Mode de coexistence

Si l'élément de services PS est fourni en mode d'approvisionnement DHCP avec le mode de coexistence et que le protocole de messagerie de gestion se révèle être SNMPv3 (voir § 6.3.6.1), l'élément de services PS DOIT alors utiliser la sécurité SNMPv3 spécifiée par RFC 3414. L'authentification SNMPv3 DOIT toujours être activée et la confidentialité SNMPv3 PEUT aussi être utilisée.

Pour l'établissement des clés SNMPv3, le câblo-modem conforme au service portail DOIT accepter "l'initialisation SNMPv3" décrite ci-dessous.

Afin de prendre en charge l'initialisation de la version SNMPv3 et les changements de clés, l'élément de services PS DOIT aussi être capable de recevoir des nuplets TLV des types 34, 34.1, et 34.2 comme défini au § B.C.1.2.8/J.112 et implémenter le mécanisme de changement de clé spécifié dans RFC 2786 qui inclut l'objet de base MIB usmDHKickstartTable.

11.3.3.1.2.1 Initialisation SNMPv3

Pour chacun des différents noms de sécurité pouvant aller jusqu'à cinq, l'autorité ultime (administrateur du service PS) produit une paire de nombres. En premier lieu, l'administrateur PS produit un nombre aléatoire Rm.

Puis l'administrateur CH utilise l'équation DH pour traduire Rm en numéro public z. L'équation est la suivante:

$$z = g \text{ ^ } Rm \text{ MOD } p$$

où g est extrait de l'ensemble des paramètres Diffie-Helman et où p est le premier de ces paramètres.

Le fichier de configuration PS inclut dès sa création la paire (nom de sécurité, numéro public). Le service PS DOIT accepter un minimum de 5 paires. Par exemple:

TLV type 34.1 (nom de sécurité de démarrage SNMPv3) = Administrateur PS

TLV type 34.2 (numéro public de démarrage SNMPv3) = z

Le service PS DOIT prendre en charge les entrées du modèle VACM définies au § 6.3.6.3. Seules les entrées VACM spécifiées dans le fichier de configuration PS par le nom de sécurité correspondant DOIVENT être actives.

Durant le processus d'amorçage du service PS, les valeurs ci-dessus (nom de sécurité, numéro public) DOIVENT être remplies dans la table usmDHKickstartTable.

A ce point:

```
usmDHKickstartMgrpublic.1 = "z" (chaîne d'octets)
usmDHKickstartSecurityName.1 = "Administrateur PS"
```

Lorsque l'objet usmDHKickstartMgrpublic.n est établi avec une valeur valide pendant l'inscription, une rangée correspondante est créée dans la table usmUserTable avec les valeurs suivantes:

```
usmUserEngineID: localEngineID
usmUserName: usmDHKickstartSecurityName.n value
usmUserSecurityName: usmDHKickstartSecurityName.n value
usmUserCloneFrom: ZeroDotZero
```

```
usmUserAuthProtocol: usmHMACMD5AuthProtocol
usmUserAuthKeyChange: (déduit de la valeur établie)
usmUserOwnAuthKeyChange: (déduit de la valeur établie)
usmUserPrivProtocol: usmDESPrivProtocol
usmUserPrivKeyChange: (déduit de la valeur établie)
usmUserOwnPrivKeyChange: (déduit de la valeur établie)
usmUserPublic
usmUserStorageType: permanent
usmUserStatus: actif
```

NOTE – Pour les entrées (PS) dhKickstart dans la table usmUserTable, "permanent" signifie qu'elles DOIVENT être écrites mais non supprimées et ne sont pas sauvegardées d'un réamorçage à l'autre.

Après que le service PS a terminé l'initialisation (ce qui est indiqué par une valeur '1' (succès) de l'objet cabhPsDevProvState):

1) le service PS génère un nombre aléatoire xa pour chaque rangée remplie de la table usmDHKickstartTable qui a un nom usmDHKickstartSecurityName et une entrée usmDHKickstartMgrPublic d'une longueur différente de zéro;

2) le service PS utilise l'équation DH pour traduire xa en numéro public c (pour chaque rangée identifiée ci-dessus):

$$c = g \text{ ^ } xa \text{ MOD } p$$

où g est extrait de l'ensemble des paramètres Diffie-Helman, p étant le premier de ces paramètres.

A ce point:

```
usmDHKickstartMyPublic.1 = "c" (chaîne d'octets)
usmDHKickstartMgrPublic.1 = "z" (chaîne d'octets)
usmDHKickstartSecurityName.1 = "Administrateur du PS"
```

3) le service PS calcule un secret partagé sk où sk = z ^ xa mod p;

4) le service PS utilise sk pour calculer la clé de confidentialité et la clé d'authentification pour chaque rangée de la table usmDHKickstartTable et établit les valeurs dans la table usmUserTable.

Comme spécifié dans le document RFC 2786, la clé de confidentialité et la clé d'authentification pour le nom d'utilisateur associé, "Administrateur PS" dans ce cas, sont déduites de sk en appliquant la fonction de déduction de clé PBKDF2 définie dans PKCS#5v2.0.

```
privacy key <---     PBKDF2 (salt = 0xd1310ba6,
                     iterationCount = 500,
                     keyLength = 16,
                     prf = id-hmacWithSHA1)
authentication key <----     PBKDF2 (salt = 0x98dfb5ac,
                     iterationCount = 500,
                     keyLength = 16 (usmHMACMD5AuthProtocol),
                     prf = id-hmacWithSHA1)
```

A ce point le service PS (portail CMP) a terminé son processus d'initialisation SNMPv3 et DOIT permettre un niveau d'accès approprié à un nom de sécurité valide avec la clé d'authentification et/ou la clé de confidentialité correcte.

Le service PS DOIT remplir correctement les tables appropriées avec les clés comme spécifié par les documents RFC se rapportant à SNMPv3 et par le document RFC 2786;

5) ce qui suit décrit le processus qu'utilise le gestionnaire pour calculer la clé d'authentification et la clé de confidentialité uniques du service PS.

Le gestionnaire SNMP accède au contenu de la table usmDHKickstartTable au moyen du nom de sécurité de l'objet "dhKickstart" sans authentification.

Le service PS DOIT fournir des entrées préinstallées dans la table du modèle USM et dans les tables du modèle VACM afin de créer correctement l'objet "dhKickstart" d'utilisateur du niveau de sécurité noAuthnoPriv qui a l'accès en lecture seule au groupe de système et à la table usmDHkickstartTable.

Si le service PS est exprimé dans le mode de coexistence et est configuré de façon à utiliser la version SNMPv3, la spécification de groupe pour la vue dhKickstart DOIT être implémentée comme suit:

```
dhKickstart Group
vacmGroupName 'dhKickstart'
vacmAccessContextPrefix ''
vacmAccessSecurityModel 3 (USM)
vacmAccessSecurityLevel NoAuthNoPriv
vacmAccessContextMatch exact
vacmAccessReadViewName 'dhKickstartView'
vacmAccessWriteViewName
vacmAccessNotifyViewName
vacmAccessStorageType permanent
vacmAccessStatus active
```

La vue du modèle VACM pour la vue dhKickstart DOIT être implémentée comme suit:

dhKickstartView: sous-arbre 1.3.6.1.2.1.1 (Groupe de système) et 1.3.6.1.3.101.1.2.1 (table usmDHkickstartTable)

Le gestionnaire SNMP obtient la valeur du numéro usmDHKickstartMyPublic du service PS associé au nom de sécurité pour lequel le gestionnaire souhaite calculer les clés d'authentification et de confidentialité. Au moyen du numéro aléatoire privé, le gestionnaire peut calculer le secret partagé à codage DH, à partir duquel il peut calculer les clés opérationnelles d'authentification et de confidentialité pour le nom de sécurité que le gestionnaire va utiliser pour communiquer avec le service PS.

11.3.3.1.2.2 Changements de clé de Diffie-Helman

Le service PS DOIT prendre en charge le mécanisme de changement de clé spécifié dans le document RFC 2786.

11.3.3.2 Algorithmes de sécurité pour SNMPv3 en mode d'approvisionnement SNMP

Si l'élément de services PS est en mode d'approvisionnement SNMP, la gestion de réseau fondée sur le protocole SNMP au sein de l'élément de services PS DOIT fonctionner en version SNMPv3 avec la sécurité spécifiée par RFC 3414. L'authentification SNMPv3 DOIT être toujours activée et la confidentialité SNMPv3 PEUT aussi être utilisée. Afin de construire les clés SNMPv3, toutes les interfaces SNMP IPCable2Home DOIVENT utiliser la gestion de clé SNMPv3 kerbérisée comme spécifié au § 11.3.3.2.3.

11.3.3.2.1 Algorithmes de chiffrement SNMPv3

Les identificateurs de transformation de chiffrement pour la gestion de clé SNMPv3 kerbérisée, DOIVENT être suivis comme défini au § 6.3.1/J.170.

11.3.3.2.2 Algorithmes d'authentification SNMPv3

Les identificateurs d'authentification pour la gestion de clé SNMPv3 kerbérisée DOIVENT être suivis comme défini au § 6.3.2/J.170.

11.3.3.2.3 Protocole SNMPv3 kerbérisé

Le profil de gestion de clé kerbérisée propre à la version SNMPv3 DOIT être suivi comme défini au § 6.5.7/J.170.

11.3.3.2.4 Identificateurs de moteur SNMPv3

Etant donné que le gestionnaire et le client SNMP DOIVENT vérifier que les identificateurs de moteur SNMPv3 contenus dans les messages de demande et de réponse AP sont fondés sur le nom du mandant approprié qui est indiqué dans le ticket Kerberos [Rec. UIT-T J.170], ce qui suit définit la règle à utiliser afin de produire ces identificateurs de moteur SNMPv3 à l'usage de la présente application:

- l'identificateur de moteur SNMPv3 suit le format définit dans RFC 2576, c'est-à-dire que le premier bit est mis à 1 (un) et que la valeur appropriée est utilisée pour les quatre premiers octets [RFC 2576];
- le cinquième octet contient la valeur 4 (quatre) afin d'indiquer que les octets suivants, jusqu'à 27, sont à considérer comme du texte. Jusqu'au 27^{e}, ces octets sont définis comme suit:
  - les 25 premiers caractères du nom de mandant Kerberos sont utilisés pour les octets d'identificateur de moteur à partir du sixième octet;
  - la séquence d'octets ci-dessus, indiquant le nom de mandant Kerberos, est suivie par un octet à considérer comme une valeur hexadécimale de 8 bits. Chaque valeur différente identifie un moteur SNMP particulier dans le dispositif (élément ou serveur de système NMS). La valeur 0 (zéro) NE DOIT PAS être utilisée;
  - la chaîne de texte qui débute au sixième octet se termine par un caractère vide.

Noter que d'autres formats sont possibles en suivant l'approche du document RFC 2576. Le choix ci-dessus cependant, est destiné à réduire la complexité d'implémentation qui serait nécessaire si toutes les approches du document RFC 2576 étaient permises.

11.3.3.2.5 Remplissage de la table usmUserTable

Les réglages de sécurité SNMPv3 pour le câblo-opérateur "CHAdministrator" en tant qu'utilisateur sont définis dans le § 6.3.6.3. L'administrateur du câble est l'autorité ultime pour la gestion de l'élément de services portail. D'autres utilisateurs peuvent également être définis. Dans le présent paragraphe, un utilisateur du modèle USM est spécifiquement défini pour le processus d'approvisionnement. Il est en particulier défini de façon à permettre de spécifier un récepteur de notification pour les messages cabhPsDevProvEnrollTrap et cabhPsDevInitTrap que le service PS est appelé à envoyer au cours du processus d'approvisionnement (voir l'étape CHPSWMD-11 du Tableau 13-1, les étapes CHPSWMS-11 et CHPSWMS-13 du Tableau 13-2 et le § 13.3.3).

Les paramètres msgSecurityParameters contenus dans les messages SNMPv3 transportent un champ msgUserName qui spécifie l'utilisateur au compte duquel le message est échangé et dont les informations de sécurité produisent les champs *msgAuthenticationParameters* et *msgPrivacyParameters*. Pour que le moteur SNMP d'un élément traite ces messages, les informations nécessaires sont appelées à être introduites dans la table *usmUserTable* [RFC 3414] pour le moteur de l'élément. La table *usmUserTable* DOIT être remplie avec les informations suivantes dans l'élément de services PS juste après la réception du message de réponse AP:

- usmUserEngineID: l'identificateur de moteur SNMP local comme défini au § 11.3.3.2.4;
- usmUserName: administrateur du service PS-XXXXXX;
- usmUserSecurityName: administrateur du service PS-XXXXXX;
- usmUserCloneFrom: 0.0;

- usmUserAuthProtocol: indique le protocole d'authentification choisi pour l'utilisateur, à partir du message de réponse AP;
- usmUserAuthKeyChange: valeur par défaut "";
- usmUserOwnAuthKeyChange: valeur par défaut "";
- usmUserPrivProtocol: indique le protocole de codage choisi pour l'utilisateur, à partir du message de réponse AP;
- usmUserPrivKeyChange: valeur par défaut "";
- usmUserOwnPrivKeyChange: valeur par défaut "";
- usmUserPublic: valeur par défaut "";
- usmUserStorageType: permanent;
- usmUserStatus: actif.

De nouveaux utilisateurs SNMPv3 PEUVENT être créés par clonage avec la norme SNMPv3 comme défini dans [RFC 3414].

La table de sécurité du modèle VACM selon le groupe [RFC 3415] DOIT être remplie avec les informations suivantes dans le service PS immédiatement après la réception du message de réponse AP:

- vacmSecurityModel: 3(usm);
- vacmSecurityName: CHAdministratorxx:xx:xx:xx:xx:xx;
- vacmGroupName: CHAdministratorSNMP;
- vacmSecurityToGroupStatus: active.

La table d'accès au modèle VACM [RFC 3415] DOIT être remplie avec les informations suivantes, associées à la table vacmSecurityToGroupTable définie ci-dessus, dans le service PS immédiatement après réception du message de réponse AP:

- vacmAccessContentPrefix: "";
- vacmAccessSecurityModel: 3(usm);
- vacmAccessSecurityLevel: AuthNoPriv;
- vacmAccessContextMatch: exact(1);
- vacmAccessReadViewName: CHAdministratorView;
- vacmAccessWriteViewName: CHAdministratorView;
- vacmAccessNotifyViewName: CHAdministratorNotifyView;
- vacmAccessStorageType: permanent;
- vacmAccessStatus: active.

Sept rangées de l'arbre de vues du modèle VACM [RFC 3415] DOIVENT être remplies avec les informations suivantes dans le service PS immédiatement après réception du message de réponse AP:

- vacmViewTreeFamilyName: CHAdministratorNotifyView;
- vacmViewTreeFamilySubtree: cabhPsDevProvEnrollTrap;
- vacmViewTreeFamilyType: inclus;
- vacmViewTreeFamilyMask: "";
- vacmViewTreeFamilyName: CHAdministratorNotifyView;
- vacmViewTreeFamilySubtree: cabhPsDevBase;
- vacmViewTreeFamilyType: inclus;

- vacmViewTreeFamilyMask: "";
- vacmViewTreeFamilyName: CHAdministratorNotifyView;
- vacmViewTreeFamilySubtree: docsDevSoftware;
- vacmViewTreeFamilyType: inclus;
- vacmViewTreeFamilyMask: "";
- vacmViewTreeFamilyName: CHAdministratorNotifyView;
- vacmViewTreeFamilySubtree: cabhPsDevInitTrap;
- vacmViewTreeFamilyType: inclus;
- vacmViewTreeFamily Mask: "";
- vacmViewTreeFamilyName: CHAdministratorNotifyView;
- vacmViewTreeFamilySubtree: cabhPsDevBase;
- vacmViewTreeFamilyType: inclus;
- vacmViewTreeFamily Mask: "";
- vacmViewTreeFamilyName: CHAdministratorNotifyView;
- vacmViewTreeFamilySubtree: docsDevEventTable;
- vacmViewTreeFamilyType: inclus;
- vacmViewTreeFamily Mask: "";
- vacmViewTreeFamilyName: CHAdministratorNotifyView;
- vacmViewTreeFamilySubtree: cabhPsDevProv;
- vacmViewTreeFamilyType: inclus;
- vacmViewTreeFamily Mask: "".

La valeur XXXXXX DOIT être l'adresse de commande MAC de réseau WAN-Man de cet élément de services PS.

De nouveaux utilisateurs du protocole SNMPv3 PEUVENT être créés par clonage normalisé avec la norme SNMPv3, comme défini dans RFC 2475. Pour des informations supplémentaires, voir le § 7.1.1.3.1/J.170.

11.3.4 CQoS sécurisée

La qualité CQoS fournit la qualité de service aux applications IPCablecom qui ont besoin d'une adresse de traversée. Les messages DQoS du modèle IPCablecom entre l'adaptateur MTA et le système CMTS, le serveur CMS ou le câblo-modem sont sécurisés par la spécification de sécurité IPCablecom. Pour la sécurité IPCable2Home, il est nécessaire de s'assurer que ces messages IPCablecom, déjà sécurisés par IPCablecom, peuvent traverser le pare-feu contenu dans l'élément de services portail (PS). Il n'est pas prévu dans le domaine d'application de la présente Recommandation d'augmenter la sécurité des messages IPCablecom. Etant donné que l'exigence de sécurité CQoS de l'élément de services PS consiste simplement à transmettre la messagerie de sécurité IPCablecom, il n'appartient pas au système NMS de prendre en charge cette fonction. En conséquence, la fonction de sécurité CQoS reste la même aussi bien pour le mode d'approvisionnement DHCP que pour le mode d'approvisionnement SNMP (voir § 5.5).

L'exigence de sécurisation de la qualité CQoS est d'offrir une sécurité qui ne soit pas une charge exagérée pour le système. Le point clé de la sécurisation de la qualité de service consiste à s'assurer que le vol de service et les interruptions du réseau soient réduits à une perte insignifiante. Il est aussi critique de comprendre que la qualité CQoS est la passerelle QS vers le réseau du domicile et qu'elle sera donc susceptible de commander ou de prendre en charge toutes les applications et tous les dispositifs résidentiels qui requièrent de la qualité de service dans le réseau câblé, vers et à

travers le service portail. Il est donc particulièrement critique de s'assurer que cet unique point d'entrée n'est pas le maillon faible dans le système de qualité de service.

11.3.4.1 Architecture de qualité CQoS

L'architecture de CQoS consiste en un élément fonctionnel de portail CQP qui facilite l'établissement des flux de qualité de service à travers le réseau HFC pour les applications IP. L'élément de portail CQP existe dans le service portail. Voir le § 10. L'élément de portail CQP agit comme un pont transparent pour la messagerie CQoS entre les applications conformes à IPCablecom et le système CMTS. Le pare-feu IPCable2Home devra être capable de transmettre la messagerie de sécurité et de qualité de service conformément au modèle IPCablecom.

Voir le § 10 pour des détails complémentaires sur la qualité CQoS.

11.3.4.2 Architecture IPCablecom de qualité DQoS sécurisée

Tableau 11-14/J.191 – Architecture de qualité DQoS sécurisée

E-MTA		
Liaison avec l'adaptateur MTA résidentiel	**Protocole**	**Protocole de sécurité**
E-MTA/CM – CMS	NCS	IPSec
E-MTA/CM – CMTS	DOCSIS	BPI+

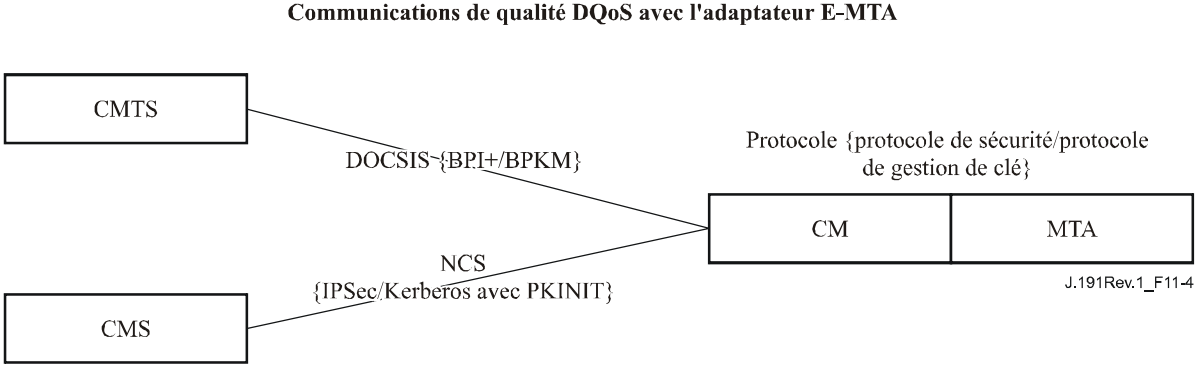


Figure 11-4/J.191 – Architecture de qualité DQoS sécurisée pour l'adaptateur MTA

11.3.4.3 Architecture de qualité CQoS de sécurité

La qualité CQoS requiert que la messagerie DQoS du modèle IPCablecom [Rec. UIT-T J.163] soit transmise à l'adaptateur E-MTA. Toute la messagerie DQoS DOIT être sécurisée comme décrit dans la spécification de sécurité IPCablecom. Le diagramme ci-dessous montre les protocoles nécessaires afin de prendre en charge l'adaptateur E-MTA pour la qualité DQoS. La seule différence entre l'architecture de qualité CQoS sécurisée et l'architecture de qualité DQoS du modèle IPCablecom est que le service portail est logiquement situé entre le câblo-modem et l'adaptateur MTA. Cependant, dans la mesure où le service portail agit comme un pont transparent, il n'y a pas de changement dans les protocoles ni dans les liaisons de communication.

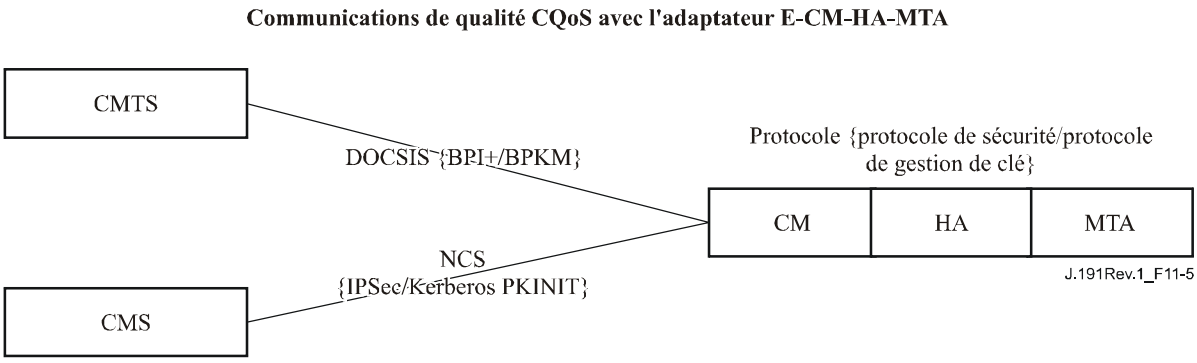


Figure 11-5/J.191 – Architecture de qualité CQoS sécurisée pour l'adaptateur MTA

11.3.4.4 Rôle du portail CSP dans la qualité CQoS

Le portail de sécurité du câble (CSP) est le point unique de contrôle de la sécurité au sein de la fonction de services portail (PS) dans le modèle IPCable2Home. Le portail CSP offre donc la sécurité dans l'architecture de qualité CQoS. Le portail CQP agit comme un pont transparent pour les messages de DQoS qu'il accepte. Le portail CSP ne fournit donc aucun service pour la qualité CQoS.

11.3.5 Gestion du pare-feu

Tandis que les questions de sécurité ont longtemps été un problème majeur pour les réseaux, l'ubiquité croissante de la connexité IP permanente au moyen d'un câblo-modem (CM) transporte les problèmes de sécurité jusqu'au domicile. Etant donné que l'abonné moyen manque de connaissances techniques, de la compréhension des questions de sécurité et du temps pour garder ses ordinateurs personnels dans le créneau supérieur du fonctionnement sécurisé, un pare-feu devient une première ligne de défense nécessaire pour protéger les ordinateurs résidentiels qui en ont besoin.

Il y a de nombreuses définitions du pare-feu, parmi lesquelles:

– "un pare-feu est une approche de la sécurité; il aide à implémenter une plus grande politique de sécurité qui définit les services et les accès à autoriser" [ICSA];

– "un pare-feu est un agent qui filtre le trafic réseau d'une certaine façon, bloquant le trafic qu'il croit être inapproprié, dangereux, ou les deux" [RFC 2979].

Un pare-feu implémente donc une politique de sécurité en se servant de certains mécanismes pour bloquer du trafic que la politique de sécurité stipule être indésirable.

Les exigences de traitement du trafic par le pare-feu sont les suivantes:

• les protocoles IPCablecom (voir Tableau 11-15) et IPCable2Home définis dans la présente Recommandation NE DOIVENT PAS être interrompus par le pare-feu. Par exemple, un pare-feu devrait avoir un mandataire spécifique d'application approprié ou un support de filtrage dynamique de paquets afin d'ouvrir les points d'accès UDP qui sont définis en application de la signalisation IPCablecom.

Tableau 11-15/J.191 – Recommandations IPCablecom applicables au pare-feu IPCable2Home

Description	Recommandation
Spécification des codecs audio/vidéo	J.161
Spécification de la qualité de service dynamique	J.163
Spécification du protocole de signalisation d'appel fourni par le réseau	J.162
Spécification de l'approvisionnement d'adaptateur MTA	J.167
Spécification de sécurité	J.170
Spécification du mécanisme d'événement de gestion	J.172
Spécification du protocole de serveur audio	J.175
Spécification de la signalisation du serveur de gestion d'appel	J.178

Les protocoles définis par IPCablecom sont les suivants:

- approvisionnement SNMPv3, DHCP, DNS, TFTP, SYSLOG
- flux média RTP, RTCP
- qualité de service RSVP
- signalisation d'appel réseau MGCP, SDP
- sécurité Messagerie Kerberos, IPSec

Les protocoles définis par IPCable2Home sont les suivants:

- approvisionnement SNMPv3, DHCP, DNS, TFTP, SYSLOG
- gestion ICMP
- sécurité Kerberos

Le pare-feu DEVRAIT protéger contre la recherche du point d'accès ou du réseau lancée de l'intérieur ou de l'extérieur du réseau du domicile. Il DEVRAIT aussi protéger contre la liste suivante d'attaques par refus de service: "Ping of Death", "Teardrop", "Bonk", "Nestea", "SYN Flood", "LAND Attack", "IP Spoofing", "Smurf Attack" et "WinNuke".

Le pare-feu DOIT être capable de permettre l'accès aux mêmes protocoles d'application Internet populaires que ceux qui sont définis à l'Annexe D. Un simple filtre de conversion NAT ou de paquets n'est pas suffisant aux fins de la présente Recommandation. Pour fournir une solution souple et sécurisée, le pare-feu DOIT implémenter soit un mandataire spécifique d'application (ASP) soit un filtrage de paquets d'après l'état (SPF).

11.3.5.1 Téléchargement à distance de l'ensemble des règles de pare-feu

Les caractéristiques de l'élément de services PS qui permettent à l'opérateur de gérer à distance les fonctions de pare-feu seront activées. Le gros de cette gestion est accompli via le téléchargement d'un fichier de configuration. Le fichier de configuration du pare-feu contient l'ensemble des règles d'une politique de sécurité particulière. La gestion de pare-feu est réalisée par l'accès aux objets de gestion de la base MIB de sécurité.

La politique de sécurité définit le niveau de sécurité/fonctionnalité désiré pour le pare-feu d'un abonné. Il peut y en avoir plusieurs à choisir. Les fichiers contenant l'ensemble des règles correspondant à ces politiques de sécurité sont conservés dans un serveur de fichiers d'opérateur. Le service portail DOIT utiliser un client TFTP conforme au document RFC 1350 afin de télécharger le fichier de configuration PS contenant l'ensemble des règles de pare-feu.

Le téléchargement du fichier de configuration du pare-feu est déclenché lors de la détection d'une différence entre la valeur utilisée pour mettre à jour (SET) l'objet MIB cabhSecFwPolicyFileURL

soit par le fichier de configuration PS ou par une commande SET du protocole SNMP, et la valeur de l'objet MIB cabhSecFwPolicySuccessfulFileURL. Si la valeur utilisée pour mettre à jour (SET) l'objet MIB cabhSecFwPolicyFileURL soit par le fichier de configuration PS ou par une commande SET du protocole SNMP, est la même que celle de l'objet MIB cabhSecFwPolicySuccessfulFileURL, le téléchargement du fichier de configuration du pare-feu NE DOIT PAS être déclenché.

La procédure de vérification de l'intégrité du fichier de configuration de pare-feu par l'élément de services PS est la suivante:

1) le générateur de fichier de configuration de pare-feu crée un hachage SHA-1 de tout le contenu de ce fichier, considéré comme une chaîne d'octets;
2) le système d'approvisionnement envoie la valeur de hachage calculée à l'étape 1 à l'élément de services PS de l'une des deux façons suivantes:
   a) modification de la valeur de l'objet MIB cabhSecFwPolicyFileHash au moyen d'un nuplet TLV de type 28 dans le fichier de configuration PS;
   b) envoi d'une commande SNMP SET afin de mettre à jour l'objet MIB cabhSecFwPolicyFileHash;
3) le système d'approvisionnement envoi le nom et l'emplacement du fichier de configuration du pare-feu afin de déclencher le téléchargement du fichier de configuration du pare-feu de l'une des deux façons suivantes:
   a) modification de la valeur de l'objet MIB cabhSecFwPolicyFileURL au moyen d'un nuplet TLV de type 28 dans le fichier de configuration PS;
   b) envoi d'une commande SNMP SET afin de mettre à jour l'objet MIB cabhSecFwPolicyFileURL;
4) si la valeur de l'objet cabhSecFwPolicyFileOperStatus n'est pas "inProgress(1)" et si la valeur utilisée pour mettre à jour (SET) l'objet MIB cabhSecFwPolicyFileURL est différente de la valeur de l'objet MIB cabhSecFwPolicySuccessfulFileURL, l'élément de services PS DOIT immédiatement télécharger le fichier désigné, à partir du serveur TFTP configuré;
5) l'élément de services PS DOIT calculer un hachage SHA-1 [FIPS 186-2] sur le contenu entier du fichier de configuration de pare-feu puis comparer ce hachage calculé avec celui qui est représenté par la valeur de l'objet MIB cabhSecFwPolicyFileHash. Si le hachage calculé et la valeur de l'objet MIB cabhSecFwPolicyFileHash sont les mêmes, l'intégrité du fichier de configuration du pare-feu est vérifiée et le fichier de configuration du pare-feu DOIT être utilisé. Sinon, le fichier DOIT être rejeté.

Un téléchargement réussi du fichier de configuration du pare-feu est défini comme étant complet après réception correcte du fichier par l'élément de services PS dans le délai de temporisation TFTP et après validation du fichier exempt d'erreur comme défini par la procédure de vérification d'intégrité ci-dessus. Après téléchargement réussi du fichier de configuration du pare-feu, le service PS DOIT mettre à jour l'objet MIB cabhSecFwPolicySuccessfulFileURL avec la même valeur que l'objet MIB cabhSecFwPolicyFileURL.

Si le téléchargement du fichier de configuration de pare-feu n'a pas réussi, le service PS NE DOIT PAS mettre à jour l'objet MIB cabhSecFwPolicySuccessfulFileURL avec la même valeur que l'objet MIB cabhSecFwPolicyFileURL. De toute façon, l'objet MIB cabhSecFwPolicyFileURL DOIT contenir la valeur mise à jour (SET) soit par le fichier de configuration PS ou par une commande SNMP SET. Lorsque le service PS est réinitialisé, l'objet MIB cabhSecFwPolicyFileURL DOIT être mis à sa valeur par défaut.

Les réglages de politique contenus dans le fichier de configuration du pare-feu DOIVENT persister d'un réamorçage à l'autre de l'élément de services PS.

L'activation et la désactivation du pare-feu du service PS sont régies par l'objet MIB cabhSecFwPolicyEnable, dont la valeur "enable(1)" indique que le pare-feu du service PS DOIT être activé après (et non avant) la détection de la valeur "pass(1)" dans l'objet MIB cabhPsDevProvState, indiquant que le processus d'approvisionnement est effectué. Cela permettra de modifier la politique de pare-feu au moyen d'un cycle d'alimentation du service PS lorsque l'accès à la gestion de réseau WAN a été accidentellement restreint. Le pare-feu du service PS NE DOIT PAS être activé si la valeur de l'objet MIB cabhSecFwPolicyEnable est "disable(2)".

L'objet MIB cabhSecFwPolicyFileCurrentVersion DOIT toujours refléter la version de la politique installée dans le service PS, qu'elle soit actuellement activée ou désactivée dans l'objet MIB cabhSecFwPolicyEnable.

11.3.5.2 Paramètres de gestion de l'ensemble de règles du pare-feu

Les paramètres de gestion suivants DOIVENT être implémentés dans le service portail comme défini par la base MIB de sécurité afin de prendre en charge le fichier d'ensemble de règles de pare-feu:

- **cabhSecFwPolicyFileURL** – cet objet contient le nom du fichier de l'ensemble de règles de politique et l'adresse IP du serveur TFTP contenant le fichier de l'ensemble de règles de politique, en format de localisation URL de protocole TFTP. Un téléchargement du fichier d'ensemble de règles de politique est déclenché lorsque la valeur utilisée pour mettre à jour (SET) cet objet de base MIB est différente de la valeur contenue dans l'objet MIB cabhSecFwPolicySuccessfulFileURL.
- **cabhSecFwPolicySuccessfulFileURL** – cet objet contient le nom du fichier de l'ensemble de règles de politique et l'adresse IP du serveur TFTP qui contenait le fichier de l'ensemble de règles de politique en format de localisation URL de protocole TFTP qui a servi à déclencher le dernier téléchargement réussi. Si un téléchargement réussi n'a pas encore eu lieu, cet objet de base MIB devrait avoir une valeur vide.
- **cabhSecFwPolicyFileHash** – cet objet définit le condensé SHA-1 pour le fichier d'ensemble de règles correspondant.
- **cabhSecFwPolicyFileOperStatus** – cet objet indique l'état du téléchargement de fichier de configuration de pare-feu et est défini comme suit: la valeur "InProgress(1)" indique qu'un téléchargement de fichier de configuration de pare-feu est en cours; la valeur "Complete(2)" indique que le fichier de configuration de pare-feu a été téléchargé et traité correctement; la valeur "Failed(4)" indique que la dernière tentative de téléchargement du fichier de configuration de pare-feu a échoué.
- **cabhSecFwPolicyFileCurrentVersion** – version du fichier d'ensemble de règles fonctionnant actuellement dans l'élément de services PS. Cet objet devrait être exprimé dans la syntaxe utilisée par le vendeur individuel afin d'identifier les versions de fichier d'ensemble de règles. L'élément de services PS DOIT renvoyer une chaîne décrivant le chargement du fichier d'ensemble de règles actuel. Si cela n'est pas applicable, cet objet DOIT contenir une chaîne vide.
- **cabhSecFwPolicyFileEnable** – cet objet permet l'activation et la désactivation de la politique de sécurité du pare-feu.

11.3.5.3 Enregistrement d'événement de pare-feu

Le pare-feu DOIT être capable d'enregistrer les types d'événement suivants:

TYPE 1: tentatives de clients aussi bien publics que privés de traverser le pare-feu en violation de la politique de sécurité.

TYPE 2: tentatives identifiées d'attaques par refus de service.

TYPE 3: changements apportés à l'un quelconque des paramètres suivants de gestion du pare-feu:

- cabhSecFwPolicyFileURL;
- cabhSecFwPolicyFileCurrentVersion;
- cabhSecFwPolicyFileEnable.

Le choix des types d'événement de pare-feu qui sont réellement enregistrés est configuré à travers l'interface de base MIB de sécurité, comme décrit au § 11.3.5.4.

Le pare-feu DOIT enregistrer les éventuels événements associés au téléchargement par TFTP du fichier de politique de pare-feu. Voir le Tableau B.1 (processus de portail CSP, sous-processus TFTP de pare-feu) dans l'Annexe B.

Les opérateurs peuvent surveiller les événements de pare-feu au moyen du mécanisme de messagerie d'événement défini au § 6.5. L'accès aux paramètres de gestion d'enregistrement d'événement se fait via la base MIB de sécurité et est défini au § 6.5.

L'enregistrement de messages d'événement de pare-feu permet à un opérateur d'évaluer le niveau d'activité des pirates dans le réseau de l'opérateur et de surveiller les changements apportés à la politique de sécurité du pare-feu. Lorsque les types de message d'événement ont été activés via les paramètres de gestion de la base MIB de sécurité, ces événements de pare-feu DOIVENT être enregistrés avec une entrée de message d'événement utilisant le mécanisme d'enregistrement d'événement défini au § 6.5.

Une entrée de message d'événement de pare-feu contiendra les informations suivantes:

- priorité d'événement;
- date et heure – d'apparition de l'événement;
- protocole – indiqué par le champ d'en-tête IP (TCP, UDP, ICMP);
- adresse IP de source;
- adresse IP de destination;
- accès de destination (TCP et UDP) ou type de message (ICMP);
- règle de politique pertinente;
- description de l'événement (facultativement).

Le § 6.5.2.1 définit un champ de priorité d'événement qui décrit différents niveaux de priorité pour les événements enregistrés. Si le champ n'est pas applicable, il doit être laissé vide. L'élément de services PS DOIT formater les messages d'événement de pare-feu comme défini à l'Annexe B.

Pour aider à la surveillance des activités de piratage sur un pare-feu d'abonné, les objets de gestion d'alerte au piratage ont été définis dans la base MIB de sécurité. Ce dispositif alerte l'opérateur lorsque le nombre d'événements de pare-feu de type 1 et de type 2 dépasse un seuil d'alerte pendant une période d'alerte donnée (en heures). Le seuil d'alerte et la période d'alerte sont configurables par l'opérateur. L'élément de services PS accumule le nombre d'événements de pare-feu de types 1 et 2 qui sont survenus pendant le nombre d'heures écoulées, défini par la période d'alerte. Si ce nombre dépasse le seuil d'alerte, un message d'alerte au piratage est enregistré pour informer l'opérateur.

11.3.5.4 Paramètres de gestion pour l'enregistrement d'événement

Les paramètres de gestion suivants DOIVENT être implémentés dans le service portail comme défini par la base MIB de sécurité pour surveiller/configurer l'enregistrement d'événement de pare-feu:

- **cabhSecFwEventType1Enable** – active ou désactive l'enregistrement de messages d'événement de pare-feu de type 1. Valeur par défaut = disable(2);

- **cabhSecFwEventType2Enable** – active ou désactive l'enregistrement de messages d'événement de pare-feu de type 2. Valeur par défaut = disable(2);
- **cabhSecFwEventType3Enable** – active ou désactive l'enregistrement de messages d'événement de pare-feu de type 3. Valeur par défaut = disable(2);
- **cabhSecFwEventAttackAlertThreshold** – si le nombre d'attaques par piratage de type 1 ou 2 dépasse ce seuil dans la période définie par l'objet cabhSecFwEventAttackAlertPeriod, un message d'événement de pare-feu DOIT être enregistré. La valeur par défaut est réglée au plus grand nombre entier autorisé. Cet objet de base MIB DOIT être ignoré si l'objet cabhSecFwEventAttackAlertPeriod est mis à 0, auquel cas un message d'événement NE DOIT PAS être envoyé. Valeur par défaut = 65535;
- **cabhSecFwEventAttackAlertPeriod** – indique la période à utiliser en heures écoulées pour l'objet cabhSecFwEventAttackAlertThreshold. Valeur par défaut = 0.

11.3.6 Bases MIB

Le service portail autonome DOIT pouvoir gérer les objets MIB de prise en charge de téléchargement de logiciel suivants, définis dans le document RFC 2669:

- **docsDevSwAdminStatus** – s'il est réglé à upgradeFromMgt(1), le dispositif initialisera un téléchargement d'image logicielle TFTP au moyen du nom docsDevSwFilename;
- **docsDevSwFilename** – nom du fichier de l'image logicielle à charger dans le dispositif;
- **docsDevSwCurrentVers** – version logicielle fonctionnant actuellement dans le dispositif;
- **docsDevSwServer** – adresse du serveur TFTP utilisé pour les mises à jour logicielles;
- **docsDevSwOperStatus** – état du téléchargement de logiciel.

Le service portail autonome DOIT pouvoir gérer les objets MIB de prise en charge de téléchargement de logiciel suivants, définis dans le document [draft-ietf-ipcdn-bpiplus-mib-12]:

- **docsBpi2CodeDownloadGroup** – collection d'objets qui servent au téléchargement de logiciels authentifiés. Le groupe docsBpi2CodeDownloadGroup inclut les objets suivants:
  - **docsBpi2CodeDownloadStatusCode** – indique le résultat de la dernière vérification de certificat CVC de fichier de configuration, de la vérification de certificat CVC par protocole SNMP, ou de la vérification de fichier de code;
  - **docsBpi2CodeDownloadStatusString** – informations complémentaires au code d'état;
  - **docsBpi2CodeMfgOrgName** – nom d'organisation du constructeur de dispositif;
  - **docsBpi2CodeMfgCodeAccessStart** – valeur actuelle de l'objet codeAccessStart du constructeur du dispositif, rapportée au temps moyen de Greenwich (GMT, *Greenwich mean time*);
  - **docsBpi2CodeMfgCvcAccessStart** – valeur actuelle de l'objet cvcAccessStart du constructeur du dispositif, rapportée au temps moyen de Greenwich (GMT);
  - **docsBpi2CodeCoSignerOrgName** – nom d'organisation du cosignataire;
  - **docsBpi2CodeCoSignerCodeAccessStart** – valeur actuelle de l'objet codeAccessStart du cosignataire, rapportée au temps moyen de Greenwich (GMT);
  - **docsBpi2CodeCoSignerCvcAccessStart** – valeur actuelle de l'objet cvcAccessStart du cosignataire, rapportée au temps moyen de Greenwich (GMT);
  - **docsBpi2CodeCvcUpdate** – déclenche la vérification par le dispositif du certificat CVC et la mise à jour de la valeur de l'objet cvcAccessStart;
- **docsBpi2CmPublicKey** – chaîne RSAPublicKey de type ASN.1 codée en règles DER, comme défini dans la norme de codage RSA [RFC 2437];
- **docsBpi2CmDeviceCmCert** – certificat X.509 de dispositif, codé en règles DER;

- **docsBpi2CmDeviceManufCert** – certificat CA X.509 de constructeur, codé en règles DER, qui a signé le certificat de dispositif.

Le service portail autonome DOIT pouvoir gérer l'objet MIB de prise en charge du téléchargement de configuration suivant:

- **cabhPsDevProvConfigHash** – hachage SHA-1 du contenu du fichier de configuration, considéré comme une chaîne d'octets. Voir § 7.3.3.

11.3.7 Téléchargement de logiciel sécurisé

Un élément de services PS autonome DOIT être capable de télécharger une image logicielle distante sur le réseau. Comme décrit au § 6.3.7, le téléchargement sécurisé de logiciels vers un service PS imbriqué est régi par le câblo-modem. La nouvelle image logicielle permettra à l'opérateur d'améliorer les performances, de fournir de nouvelles fonctions et caractéristiques, de corriger des déficiences de conception, et d'offrir un chemin de migration aux dispositifs IPCable2Home lors des évolutions de la présente Recommandation. La capacité de télécharger des logiciels DOIT permettre de changer les fonctionnalités de l'élément de services PS sans qu'il soit besoin que le personnel du système câblé visite physiquement et reconfigure chaque unité. Le processus de téléchargement de logiciel sécurisé du service PS autonome vise les exigences primaires de système suivantes:

- Le mécanisme utilisé pour télécharger des logiciels DOIT être le protocole de transfert de fichier TFTP.
- Le téléchargement de logiciel DOIT être initialisé de l'une des deux façons suivantes:
  1) via une demande SNMP de mise à jour envoyée par le système NMS à l'objet docsDevSwAdminStatus;
  2) via le fichier de configuration PS de l'élément de services PS.

  Si le nom de fichier de mise à jour logicielle contenu dans le fichier de configuration PS ne correspond pas à l'image logicielle actuelle du dispositif, l'élément de services PS DOIT demander le fichier spécifié via TFTP auprès du serveur de logiciel.
- L'élément de services PS DOIT vérifier que l'image logicielle téléchargée est appropriée pour lui-même. Si l'image logicielle téléchargée est appropriée, l'élément de services PS DOIT écrire la nouvelle image logicielle dans une mémoire non volatile. Une fois que le transfert du fichier est terminé et réussi, le dispositif DOIT se redémarrer avec la nouvelle configuration.
- Si l'élément de services PS n'est pas en mesure de terminer le transfert de fichier pour une raison quelconque, l'élément de services PS DOIT rester capable d'accepter de nouveaux téléchargements de logiciel (sans interaction avec l'opérateur ou avec l'utilisateur), même si l'alimentation ou la connexité est interrompue entre les essais.
- L'élément de services PS DOIT enregistrer les échecs de téléchargement et PEUT les signaler de manière asynchrone au gestionnaire de réseau.
- Lorsque le logiciel a été amélioré pour satisfaire à une nouvelle version de la présente Recommandation, le logiciel DOIT impérativement alors travailler avec la version précédente afin de permettre une transition graduelle des unités sur le réseau.
- L'élément de services PS DOIT authentifier l'initiateur du téléchargement de logiciel.
- L'élément de services PS DOIT vérifier que le code téléchargé n'a pas été altéré par rapport à la forme originale dans laquelle il a été fourni par la source habilitée.
- Le processus de téléchargement de logiciel DOIT fournir à un opérateur les mécanismes de surclassement/repli de la version de code des éléments IPCable2Home.
- Le processus de téléchargement de logiciel DOIT offrir des options permettant à un opérateur de définir ses propres politiques de téléchargement.

- Le constructeur du fichier de code DOIT appliquer une signature de vérification de code (CVS) à l'image du code et à tous autres attributs authentifiés, comme défini dans la présente Recommandation pour la signature numérique de la structure PKCS#7 appliquée au fichier de code; la clé privée utilisée pour appliquer la signature DOIT être liée à un certificat de clé publique qui permet de suivre la chaîne jusqu'au certificat CVC racine. La signature du constructeur authentifie la source et l'intégrité du fichier de code.
- Un cosignataire (opérateur ou service portail) PEUT contresigner le fichier de code en plus de la signature du constructeur.
- L'élément de services PS DOIT être capable de traiter une signature numérique PKCS#7 et un certificat IPCable2Home selon X.509 comme défini aux § 11.3.7.2.1.1 et 11.3.7.3 respectivement.
- (Facultatif): l'élément de services PS DEVRAIT être capable de mettre à jour le certificat CA racine de CVC, mémorisé dans le dispositif.
- (Facultatif): l'élément de services PS DEVRAIT être capable de remplacer le ou les certificats CA de constructeur, mémorisés dans le dispositif.
- (Facultatif): l'élément de services PS DEVRAIT être capable de mettre à jour le certificat CA de CVC, mémorisé dans le dispositif.
- (Facultatif): l'élément de services PS DEVRAIT être capable de mettre à jour le certificat CA racine de fournisseur de services, mémorisé dans le dispositif.

Le téléchargement facultatif du certificat racine de fournisseur de services, du certificat CA racine de CVC, du certificat CA de CVC, et/ou du certificat CA de constructeur en tant que partie du fichier de code permet de distinguer clairement l'image de code des autres paramètres contenus dans le fichier de téléchargement de code. Il est possible de changer le certificat CA racine du fournisseur de services, le certificat CA racine de CVC, le certificat CA de CVC et/ou le certificat CA de constructeur interprété par l'élément de services PS en insérant ces nouveaux certificats dans l'image du code. L'insertion du certificat CVC de constructeur et/ou d'un certificat CVC de cosignataire avec la signature CVS correspondante permet à l'élément de services PS de vérifier que l'image de code n'a pas été altérée depuis que le certificat CA racine de fournisseur de services, le certificat CA racine de CVC, le certificat CA de CVC et/ou le certificat CA de constructeur ou des paramètres SignedData ont été annexés à l'image de code.

11.3.7.1 Téléchargement de logiciel vers les éléments de services portail imbriqués ou autonomes

Comme indiqué dans la Figure 11-6 ci-dessous, un dispositif d'accès résidentiel (HA) complet peut implémenter le câblo-modem et l'élément de services PS en tant qu'entités distinctes ou en tant qu'entités imbriquées, comme défini dans le § 5.1.3.1.

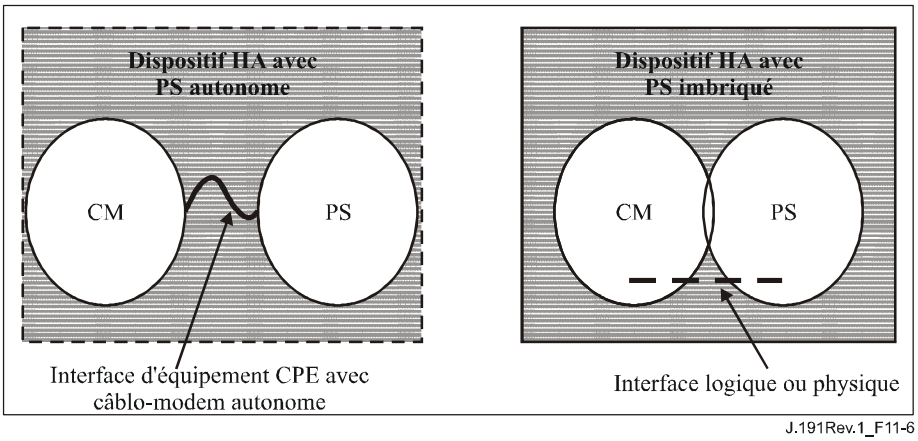


Figure 11-6/J.191 – Dispositif HA

Dans le modèle IPCable2Home:

- si l'élément de services PS est imbriqué avec un câblo-modem, l'image PS/CM DOIT être une image unique et le téléchargement de logiciel ne DOIT être effectué que par le câblo-modem;
- si l'élément de services PS est composé d'entités autonomes distinctes, le téléchargement de logiciel pour les éléments IPCable2Home DOIT être effectué par l'élément de services PS comme décrit ci-dessous.

11.3.7.2 Exigences relatives au fichier de code

11.3.7.2.1 Structure du fichier de téléchargement de code pour le téléchargement de logiciel sécurisé

Pour un téléchargement de logiciel sécurisé, le fichier de téléchargement de code est un fichier construit au moyen d'une structure conforme à RFC 2315 qui a été définie dans un format spécifique de l'utilisation avec des éléments de services portail. Le fichier de code DOIT se conformer à RFC 2315 et DOIT être codé conformément aux règles DER. Le fichier de code DOIT correspondre à la structure indiquée au Tableau 11-16.

Lorsque des certificats sont téléchargés en tant que partie du fichier de code, ces certificats PEUVENT être contenus dans les champs spécifiés dans le Tableau 11-16, et être séparés de l'image de code réelle contenue dans le champ CodeImage.

Tableau 11-16/J.191 – Structure du fichier de code

Fichier de code	Description
PKCS#7 Digital Signature {	
ContentInfo	
ContentType	SignedData
SignedData ()	Valeur EXPLICITE du contenu des données signées: y compris la signature CVS et les signatures CVS conformes à X.509
} fin de signature numérique PKCS#7	

Tableau 11-16/J.191 – Structure du fichier de code

Fichier de code	Description
SignedContent {	
Download Parameters {	Format de TLV obligatoire (type 28). (La longueur est zéro s'il n'y a pas de sous-TLV.)
MfgCACerts ()	Nuplet TLV facultatif pour un ou plusieurs certificat(s) à codage DER dont chacun est formaté conformément au nuplet TLV de certificat CA de constructeur (type 17).
clabServProvRootCACert ()	Nuplet TLV facultatif pour un certificat à codage DER formaté conformément au nuplet TLV de certificat CA racine de fournisseur de services (type 50).
clabCVCRootCACert ()	Nuplet TLV facultatif pour un certificat à codage DER formaté conformément au nuplet TLV de certificat CA racine de CVC (type 51).
clabCVCCACertificate ()	Nuplet TLV facultatif pour un certificat à codage DER formaté conformément au nuplet TLV de certificat CA de CVC (type 52).
}	
CodeImage ()	Image du code de mise à jour.
} *fin de SignedContent*	

11.3.7.2.1.1 Données signées

Le fichier de téléchargement de code contiendra les informations avec un type de contenu de données signées [RFC 2315] comme indiqué ci-dessous dans le Tableau 11-17. Tout en maintenant la conformité à RFC 2315, la structure utilisée a été réduite en terme de format afin de faciliter le traitement effectué par le service portail en vue de valider la signature. Les données signées [RFC 2315] DOIVENT être codées en règles DER et correspondre exactement à la structure indiquée ci-dessous sauf pour les éventuels changements d'ordre requis par le codage DER (par exemple l'ordre des attributs de type SET OF). L'élément de services PS DEVRAIT rejeter la signature [RFC 2315] si les données signées [RFC 2315] ne correspondent pas à la structure codée en règles DER.

Tableau 11-17/J.191 – Données signées PKCS#7

Champ PKCS#7	Description
Signed Data {	
version	Version = 1
DigestAlgorithmIdentifiers	SHA-1
ContentInfo	
ContentType	Données (l'élément SignedContent est concaténé à la fin de la structure PKCS#7)
certificates {	(Certificat de vérification de code (CVC) de CableLabs)
mfgCVC	(EXIGE pour tous les fichiers de code)
co-signerCVC	(FACULTATIF; exigé pour les cosignatures)
} *fin des certificats*	

Tableau 11-17/J.191 – Données signées PKCS#7

Champ PKCS#7	Description
SignerInfo{	
MfgSignerInfo {	(EXIGE pour tous les fichiers de code)
version	Version = 1
issuerAndSerialNumber	
issuerName	
CountryName	USA
organizationName	CableLabs
CommonName	CA racine de CVC de CableLabs
certificateSerialNumber	<Numéro de série de CVC Mfg>
digestAlgorithm	SHA-1
AuthenticatedAttributes	
contentType	Données (type de contenu de l'élément signedContent)
signingTime	Temps UTC (GMT), AAMMJJhhmmssZ
messageDigest	(Condensé du contenu comme défini dans [PKCS#7])
digestEncryptionAlgorithm	Chiffrement RSA
EncryptedDigest	
} *fin des infos de signataire mfg*	
CoSignerInfo {	(FACULTATIF; exigé pour les cosignatures)
version	Version = 1
issuerAndSerialNumber	
issuerName	
CountryName	USA
organizationName	CableLabs
CommonName	CA racine de CVC de CableLabs
certificateSerialNumber	<Numéro de série de CVC de cosignataire>
digestAlgorithm	SHA-1
AuthenticatedAttributes	
contentType	Données (type de contenu de l'élément signedContent)
signingTime	Temps UTC (GMT), AAMMJJhhmmssZ
messageDigest	(Condensé du contenu comme défini dans [PKCS#7]
digestEncryptionAlgorithm	Chiffrement RSA
EncryptedDigest	
} *fin des infos de signataire mso*	
} *fin des infos de signataire*	
} *fin des données signées*	

11.3.7.2.1.2 Contenu signé

Le champ de contenu signé du fichier de code contient l'image du code et le champ des paramètres de téléchargement, qui peut éventuellement contenir d'autres éléments facultatifs supplémentaires – un certificat CA racine de fournisseur de services, un certificat CA racine de CVC de laboratoire d'essais de certification (CTL, *certification testing laboratory*), un certificat CA de CVC de laboratoire CTL et/ou le certificat CA du constructeur.

L'image de code finale est exprimée en un format compatible avec l'élément de services PS de destination. Afin de prendre en charge les exigences relatives à la signature PKCS#7, le contenu du code est caractérisé comme des données, c'est-à-dire comme une simple chaîne d'octets. Le format de l'image de code finale n'est pas spécifié ici et sera défini par chaque constructeur en fonction de ses exigences.

Chaque constructeur DEVRAIT construire son code avec des mécanismes supplémentaires qui vérifient qu'une image de code améliorée est compatible avec l'élément de services PS de destination.

S'il est inclus dans le champ de contenu signé, un certificat est destiné à remplacer le certificat actuellement mémorisé dans l'élément de services PS. Si le téléchargement et l'installation du code sont réussis, l'élément de services PS DOIT alors remplacer son certificat actuellement mémorisé par le nouveau certificat reçu dans le champ de contenu signé. Ce nouveau certificat sera alors utilisé pour les vérifications subséquentes.

11.3.7.2.1.3 Clés de signature de code

La signature numérique [RFC 2315] utilise l'algorithme de chiffrement RSA [RFC 2437] avec hachage SHA-1 [FIPS 186-2]. L'élément de services PS DOIT être capable de vérifier les signatures de fichier de code. L'exposant public est F_4 (65 537 en décimal).

11.3.7.2.1.4 Certificat CA de constructeur

Cet attribut est une chaîne contenant un certificat CA X.509, comme défini dans la Rec. UIT-T X.509 | ISO/CEI 9594-8.

Type	Longueur	Valeur
17	Variable	Certificat CA X.509 (ASN.1 à codage DER)

11.3.7.2.1.5 Certificat CA racine de fournisseur de services

Cet attribut est une chaîne contenant un certificat CA racine de fournisseur de services X.509, comme défini dans la Rec. UIT-T X.509 | ISO/CEI 9594-8. Ce certificat peut être utilisé par l'élément de services PS en mode d'approvisionnement SNMP pour l'authentification mutuelle.

Type	Longueur	Valeur
50	Variable	Certificat CA X.509 (ASN.1 à codage DER)

11.3.7.2.1.6 Certificat CA racine de CVC

Cet attribut est une chaîne contenant un certificat CA racine de CVC X.509, comme défini dans la Rec. UIT-T X.509 | ISO/CEI 9594-8. Ce certificat peut être utilisé par l'élément de services PS autonome au cours du processus de téléchargement de logiciel sécurisé.

Type	Longueur	Valeur
51	Variable	Certificat CA X.509 (ASN.1 à codage DER)

11.3.7.2.1.7 Certificat CA de CVC

Cet attribut est une chaîne contenant un certificat CA de CVC X.509, comme défini dans la Rec. UIT-T X.509 | ISO/CEI 9594-8. Ce certificat peut être utilisé par l'élément de services PS autonome au cours du processus de téléchargement de logiciel sécurisé.

Type	Longueur	Valeur
52	Variable	Certificat CA X.509 (ASN.1 à codage DER)

11.3.7.3 Format de certificat de vérification de code (CVC)

11.3.7.3.1 Format de CVC pour le téléchargement de logiciel sécurisé

Pour le téléchargement de logiciel sécurisé, le format utilisé pour le certificat CVC est conforme à X.509. Cependant, la structure X.509 a été réduite afin de faciliter le traitement effectué par un élément de services PS pour valider le certificat et extraire la clé publique utilisée afin de vérifier la signature CVS. Le certificat CVC DOIT être codé en règles DER et correspondre exactement à la structure indiquée au Tableau 11-18 sauf pour les changements d'ordre requis par le codage DER (par exemple l'ordre des attributs SET OF). L'élément de services PS DEVRAIT rejeter le certificat CVC s'il ne correspond pas à la structure codée en règles DER représentée au Tableau 11-18. Le codage DER DOIT satisfaire aux exigences du § 11.3.2.

Tableau 11-18/J.191 – Certificat de vérification de code conforme à la Rec. UIT-T X.509

Certificat X.509	Description
Certificate {	
version	2 (c'est-à-dire X.509 version 3)
serialNumber	Entier, 20 octets (c'est-à-dire, nombre unique attribué par l'autorité CA racine)
signature	RSA SHA-1, paramètres vides
issuer	
countryName	USA
organizationName	
commonName	Certificat CA racine de CVC
validity	
notBefore	Temps UTC (GMT), AAMMJJhhmmssZ (c'est-à-dire l'heure de la production)
notAfter	Temps UTC (GMT), AAMMJJhhmmssZ
subject	
countryName	<Nom du pays>
organizationName	<Nom de l'entreprise>
commonName	<Nom courant>
subjectPublicKeyInfo	
algorithm	Chiffrement RSA, paramètres vides
subjectPublicKey	Module de 2048 bits

Tableau 11-18/J.191 – Certificat de vérification de code conforme à la Rec. UIT-T X.509

Certificat X.509	Description
extensions	
KeyUsage	<Utilisation de la clé>
authorityKeyIdentifier	<Identificateur de la clé d'autorité>
signatureAlgorithm	RSA SHA-1, paramètres vides
signatureValue	<Valeur de la signature>
} *fin de certificat*	

11.3.7.3.2 Révocation de certificat

La présente Recommandation n'exige pas ou ne définit pas l'utilisation de listes de révocation de certificat (CRL). Il n'est pas demandé à l'élément de services PS de traiter les listes CRL. Les opérateurs peuvent vouloir définir et utiliser les listes CRL en dehors du réseau HFC pour aider à la gestion des fichiers de code qui leur sont fournis par les constructeurs. Cependant, il existe une méthode de révocation des certificats fondée sur la date de début de validité du certificat. Cette méthode exige qu'un certificat CVC mis à jour soit délivré à l'élément de services PS avec une heure de début de validité mise à jour. Une fois que la validation du certificat CVC a réussi, l'heure de début de validité X.509 va mettre à jour la valeur actuelle de l'objet cvcAccessStart de l'élément de services PS.

11.3.7.4 Contrôles d'accès de fichier de code

Pour le téléchargement de logiciel sécurisé, des valeurs de contrôle spéciales sont incluses dans le fichier de code pour que l'élément de services PS les vérifie avant qu'il ne valide une image de code. Les conditions imposées aux valeurs de ces paramètres de contrôle DOIVENT être satisfaites avant que l'élément de services PS valide le certificat CVC ou la signature CVS et accepte l'image de code.

11.3.7.4.1 Noms d'organisation titulaire

L'élément de services PS va reconnaître jusqu'à deux noms, à tout instant donné, qu'il considère comme un agent signataire de code autorisé dans le champ de titulaire d'un certificat CVC de fichier de code. Ces deux noms sont les suivants:

- le constructeur du dispositif: le nom du constructeur figurant dans le champ de titulaire du certificat CVC du constructeur DOIT correspondre exactement au nom du constructeur mémorisé dans une mémoire non volatile de l'élément de services PS par le constructeur. Un certificat CVC de constructeur DOIT toujours être inclus dans le fichier de code;
- un agent cosignataire: il est permis qu'une autre organisation autorisée cosigne les fichiers de code destinés au dispositif. Dans la plupart des cas, c'est l'opérateur qui contrôle le domaine de fonctionnement actuel du dispositif. Le nom d'organisation du cosignataire est communiqué à l'élément de services PS via un certificat CVC du cosignataire inséré dans le fichier de configuration PS lors de l'initialisation du processus de vérification de code de l'élément de services PS. Le nom d'organisation du cosignataire figurant dans le champ de titulaire CVC du cosignataire DOIT correspondre exactement au nom d'organisation du cosignataire reçu précédemment dans le certificat CVC d'initialisation du cosignataire et mémorisé par l'élément de services PS.

L'élément de services PS PEUT comparer les noms d'organisation au moyen d'une comparaison binaire.

11.3.7.4.2 Contrôles variables dans le temps

Pour atténuer la possibilité qu'un élément de services PS reçoive un précédent fichier de code via une attaque par répétition, les fichiers de code incluent une valeur d'heure signée dans la structure PKCS#7 qui peut servir à indiquer l'heure de signature de l'image de code. L'élément de services PS DOIT conserver deux valeurs de temps UTC associées à chaque agent de signature de code. Un seul ensemble DOIT toujours être mémorisé et entretenu pour le constructeur du dispositif. De plus, si le fichier de code est cosigné, l'élément de services PS DOIT aussi mémoriser et entretenir un ensemble séparé de valeurs temporelles pour le cosignataire.

Ces valeurs servent à contrôler l'accès du fichier de code à l'élément de services PS en contrôlant individuellement la validité de la signature CVS et le certificat CVC. Ces valeurs sont les suivantes:

- codeAccessStart: valeur temporelle UTC de 12 octets se rapportant au temps moyen de Greenwich (GMT).
- cvcAccessStart: valeur temporelle UTC de 12 octets se rapportant au temps moyen de Greenwich (GMT).

Les valeurs du temps UTC incluses dans le certificat CVC DOIVENT être exprimées en temps GMT et DOIVENT inclure les secondes, c'est-à-dire qu'elles DOIVENT être exprimées dans le format suivant: AAMMJJhhmmssZ. Le champ d'année (AA) DOIT être interprété comme suit:

- lorsque AA est supérieur ou égal à 50, l'année doit être interprétée comme 19AA;
- lorsque AA est inférieur à 50, l'année doit être interprétée comme 20AA.

Ces valeurs feront toujours référence au temps moyen de Greenwich, de sorte que le caractère ASCII (Z) final peut être supprimé lorsqu'elles sont mémorisées par l'élément de services PS dans les objets codeAccessStart et cvcAccessStart.

L'élément de services PS DOIT entretenir chacune de ces valeurs de temps dans un format qui contienne les informations de temps équivalentes et applicables au format UTC à 12 caractères (c'est-à-dire, AAMMJJhhmmss). L'élément de services PS DOIT comparer précisément ces valeurs mémorisées avec les valeurs de temps UTC délivrées par l'élément de services PS dans un certificat CVC. Ces exigences seront examinées plus bas dans la présente Recommandation.

Les valeurs des objets codeAccessStart et cvcAccessStart correspondant au constructeur de l'élément de services PS NE DOIVENT PAS décroître. La valeur des objets codeAccessStart et cvcAccessStart correspondant au cosignataire NE DOIT PAS décroître tant que le cosignataire ne change pas et que l'élément de services PS maintient ces valeurs de contrôle variables dans le temps du cosignataire.

11.3.7.5 Initialisation de mise à jour de code

11.3.7.5.1 Initialisation du constructeur

Il appartient au constructeur d'installer correctement la version initiale de code dans l'élément de services PS.

Afin de prendre en charge le téléchargement de logiciel sécurisé, les valeurs des contrôle variables dans le temps DOIVENT être chargées dans une mémoire non volatile de l'élément de services PS:

- nom d'organisation du constructeur de l'élément de services PS;
- valeurs des contrôles variables dans le temps du constructeur:
  a) valeur d'initialisation de l'objet codeAccessStart;
  b) valeur d'initialisation de l'objet cvcAccessStart.

Le nom d'organisation du constructeur de l'élément de services PS DOIT toujours être présent dans le dispositif. Le nom d'organisation du constructeur de l'élément de services PS PEUT être mémorisé dans l'image de code du dispositif. Le nom du constructeur utilisé pour la mise à jour du code n'est pas nécessairement le même que celui qui est utilisé dans le certificat CA de constructeur.

Les valeurs de contrôles variables dans le temps, objets codeAccessStart et cvcAccessStart, DOIVENT être initialisées à un temps UTC compatible avec l'heure de début de validité du dernier certificat CVC du constructeur. Ces valeurs variables dans le temps seront mises à jour périodiquement en période de fonctionnement normal au moyen des certificats CVC du constructeur qui sont reçus et vérifiés par l'élément de services PS.

Le constructeur DOIT initialiser les certificats suivants dans la mémoire non volatile de l'élément de services PS autonome:

- certificat CA racine de fournisseur de services;
- certificat CA racine de CVC;
- certificat CA de CVC;
- certificat CA de constructeur;
- certificat de l'élément de services PS.

Le constructeur DOIT initialiser les certificats suivants dans la mémoire non volatile de l'élément de services PS imbriqué:

- certificat CA racine de fournisseur de services;
- certificat CA de constructeur;
- certificat de l'élément de services PS.

11.3.7.5.2 Initialisation du réseau

Pour les besoins de la vérification de code, le fichier de configuration PS est utilisé comme moyen authentifié dans lequel on initialise le processus de vérification de code. Dans le fichier de configuration PS de l'élément de services PS, celui-ci reçoit les réglages de configuration pertinents pour la vérification de mise à jour de code.

Le fichier de configuration PS DEVRAIT toujours inclure le certificat CVC le plus à jour applicable à l'élément de services PS de destination; mais lorsque le fichier de configuration PS sert à initialiser une mise à jour de code, il DOIT inclure un certificat de vérification de code (CVC) pour initialiser l'acceptation des fichiers de code par l'élément de services PS conformément à la présente Recommandation. Qu'une mise à jour de code soit ou non nécessaire, un certificat CVC contenu dans le fichier de configuration PS DOIT être traité par l'élément de services PS. Un fichier de configuration PS PEUT contenir:

- aucun certificat CVC – l'élément de services PS NE DOIT PAS accepter de fichier de code;
- seulement un certificat CVC de constructeur – l'élément de services PS DOIT vérifier que le certificat CVC de constructeur s'articule bien jusqu'à la racine de certificat CVC avant d'accepter un fichier de code. Lorsque le fichier de configuration PS de l'élément de services PS ne contient qu'un certificat CVC de constructeur valide, le dispositif ne demande alors qu'une signature de constructeur sur les fichiers de code. Dans ce cas, l'élément de services PS NE DOIT PAS accepter de fichiers de code qui n'ont pas été cosignés;
- seulement un certificat CVC de cosignataire – l'élément de services PS DOIT vérifier que le certificat CVC du cosignataire s'articule bien jusqu'à la racine de certificat CVC avant d'accepter un fichier de code. Lorsque le fichier de configuration PS de l'élément de services PS contient un certificat CVC de cosignataire valide, il est utilisé pour initialiser le dispositif avec un cosignataire. Une fois validé, le nom organizationName du titulaire du

certificat CVC deviendra le cosignataire de code attribué à l'élément de services PS. Pour qu'un élément de services PS accepte ultérieurement une image de code, le cosignataire DOIT avoir signé le fichier de code en plus du constructeur du dispositif IPCable2Home;

- à la fois un certificat CVC de constructeur et un certificat CVC de cosignataire. L'élément de services PS DOIT vérifier que les deux certificats CVC s'articulent bien jusqu'à la racine de certificats CVC avant d'accepter un fichier de code.

Avant que l'élément de services PS active sa capacité de mise à jour des fichiers de code sur le réseau, il DOIT recevoir un certificat CVC valide dans un fichier de configuration. De plus, lorsque le fichier de configuration PS de l'élément de services PS ne contient pas de certificat CVC valide et que sa capacité à mettre à jour les fichiers de code a été désactivée, l'élément de services PS DOIT rejeter toute information contenue dans un certificat CVC délivré ultérieurement via SNMP.

Le nom d'organisation du constructeur de l'élément de services PS et les valeurs de contrôle variables dans le temps du constructeur DOIVENT être présents dans l'élément de services PS. Si celui-ci est initialisé afin de prendre en charge un code cosigné par un cosignataire supplémentaire, le nom de l'organisation et les valeurs correspondantes de contrôle variables dans le temps DOIVENT être mémorisées et entretenues pendant qu'elles sont opérationnelles. De l'espace DOIT être attribué dans la mémoire de l'élément de services PS pour les valeurs de contrôle de cosignataires suivantes:

1) nom d'organisation de l'agent cosignataire;
2) valeurs de contrôle variables dans le temps du cosignataire:
   a) cvcAccessStart
   b) codeAccessStart

L'ensemble de ces valeurs du constructeur DOIT être mémorisé dans la mémoire non volatile de l'élément de services PS et ne doit pas être perdu lorsque la source d'alimentation principale du dispositif est supprimée ou lors d'un réamorçage.

Lorsqu'un cosignataire est attribué à l'élément de services PS, l'ensemble de valeurs de certificat CVC du cosignataire DOIT être mémorisé par l'élément de services PS, lequel PEUT retenir ces valeurs dans une mémoire non volatile qui ne doit pas être perdue lorsque la source d'alimentation principale du dispositif est supprimée ou lors d'un réamorçage. Cependant, lors de l'attribution d'un cosignataire à un élément de services PS, le certificat CVC est toujours dans le fichier de configuration. L'élément de services PS recevra donc toujours les valeurs de contrôle du cosignataire pendant la phase d'initialisation et il ne lui est donc pas imposé de mémoriser les valeurs de contrôle variables dans le temps lorsque l'alimentation du secteur est perdue ou pendant un processus de réamorçage.

11.3.7.6 Traitement de certificat CVC

Pour accélérer la livraison d'un certificat CVC mis à jour sans demander au service portail de procéder à la mise à jour de code, le certificat CVC PEUT être livré soit dans le fichier de configuration PS ou dans une base MIB du protocole SNMP. Le format du certificat CVC est le même qu'il soit un fichier de code, un fichier de configuration PS ou une base MIB du protocole SNMP.

11.3.7.6.1 Traitement du certificat CVC du fichier de configuration

Lorsqu'un certificat CVC est inclus dans le fichier de configuration, l'élément de services PS DOIT vérifier ce certificat CVC avant d'accepter l'un quelconque des réglages de mise à jour de code qu'il contient. Dès réception du certificat CVC dans le fichier de configuration, l'élément de services PS DOIT effectuer les étapes de validation et de procédure suivantes. Si l'un des essais de vérification suivants échoue, l'élément de services PS DOIT immédiatement arrêter le processus de vérification du certificat CVC et enregistrer l'erreur s'il y a lieu. Si le fichier de configuration PS de l'élément de

services PS n'inclut pas de certificat CVC correctement validé, l'élément de services PS NE DOIT PAS télécharger de fichiers de mise à jour de code, qu'ils soient déclenchés par le fichier de configuration PS de l'élément de services PS ou via une base MIB du protocole SNMP. De plus, si les fichiers de configuration de l'élément de services PS n'incluent pas de certificat CVC correctement validé, l'élément de services PS n'est pas tenu de traiter les certificats CVC délivrés ultérieurement via une base MIB du protocole SNMP et NE DOIT PAS accepter d'informations d'un certificat CVC ultérieurement délivré via une base MIB du protocole SNMP.

Dès réception du certificat CVC dans un fichier de configuration, l'élément de services PS DOIT:

1) vérifier que l'extension d'utilisation de clé étendue est exprimée en le certificat CVC comme défini au § 11.3.2.2.2;

2) vérifier le nom d'organisation titulaire de certificat.

   a) Si le certificat CVC est un certificat CVC de constructeur (Type 32), alors:

      i) SI le nom d'organisation est identique au nom de constructeur du dispositif, ALORS c'est le certificat CVC du constructeur. Dans ce cas, l'élément de services PS DOIT vérifier que la date de début de validité du certificat CVC de constructeur est supérieure ou égale à la valeur cvcAccessStart du constructeur actuellement contenue dans l'élément de services PS;

      ii) SI le nom d'organisation n'est pas identique au nom de constructeur du dispositif, ce certificat CVC DOIT ALORS être rejeté et l'erreur doit être enregistrée.

   b) Si le certificat CVC est un certificat CVC de cosignataire (Type 33) alors:

      i) SI le nom d'organisation est identique au cosignataire de code actuel de l'élément de services PS, ALORS c'est le certificat CVC du cosignataire actuel et l'élément de services PS DOIT vérifier que la date de début de validité est supérieure ou égale à la valeur cvcAccessStart du cosignataire actuellement contenue dans l'élément de services PS;

      ii) SI le nom d'organisation n'est pas identique au nom de cosignataire actuel, ALORS, après que le certificat CVC a été validé (et que l'enregistrement est terminé) ce nom d'organisation titulaire deviendra le nouveau cosignataire de code de l'élément de services PS, lequel NE DOIT PAS accepter de fichier tant qu'il n'a pas été signé par le constructeur et cosigné par le cosignataire de code;

3) valider la signature de l'émetteur de certificat CVC en utilisant la clé publique CA de certificat CVC de laboratoire CTL détenue par l'élément de services PS;

4) valider la signature CA de certificat CVC de laboratoire CTL en utilisant la clé publique CA racine de CVC de laboratoire CTL détenue par l'élément de services PS. La vérification de la signature authentifiera la source et validera la confiance dans les paramètres de certificat CVC;

5) mettre à jour la valeur actuelle cvcAccessStart de l'élément de services PS correspondant au nom d'organisation du certificat CVC (c'est-à-dire du constructeur ou du cosignataire) avec la valeur de date de début de validité venant du certificat CVC validé. Si la valeur de date de début de validité est supérieure à la valeur actuelle de l'objet codeAccessStart de l'élément de services PS, mettre à jour la valeur de l'objet codeAccessStart de l'élément de services PS avec la valeur de date de début de validité. L'élément de services PS DEVRAIT ignorer tous les résidus du certificat CVC.

11.3.7.6.2 Traitement du certificat CVC par protocole SNMP

L'élément de services PS DOIT traiter les certificats CVC livrés par le protocole SNMP lorsqu'il a la capacité de mettre à jour les fichiers de code; sinon, tous les certificats CVC livrés via le protocole SNMP DOIVENT être rejetés. Lorsqu'il valide le certificat CVC livré via SNMP, l'élément de services PS DOIT effectuer les étapes de validation et de procédure suivantes. Si l'un

quelconque des essais de vérification suivants échoue, l'élément de services PS DOIT immédiatement arrêter le processus de vérification de certificat CVC, enregistrer s'il y a lieu l'erreur et supprimer tous les résidus du processus de cette étape.

L'élément de services PS DOIT:

1) vérifier que l'extension d'utilisation de clé étendue est contenue dans ce certificat CVC comme défini au § 11.3.2.2.2;

2) vérifier le nom d'organisation titulaire du certificat CVC;

   a) SI le nom d'organisation est identique au nom de constructeur du dispositif, ALORS c'est le certificat CVC du constructeur. Dans ce cas, l'élément de services PS DOIT vérifier que la date de début de validité du certificat CVC du constructeur est supérieure à la valeur de l'objet cvcAccessStart du constructeur actuellement contenue dans l'élément de services PS;

   b) SI le nom d'organisation est identique au cosignataire de code actuel de l'élément de services PS, ALORS c'est un certificat CVC actuel de cosignataire, et la date de début de validité DOIT être supérieure à la valeur de l'objet cvcAccessStart du cosignataire actuellement contenue dans l'élément de services PS;

   c) SI le nom d'organisation n'est pas identique au nom du constructeur de dispositif ou du cosignataire actuel, ALORS l'élément de services PS DOIT immédiatement rejeter ce certificat CVC;

3) valider la signature de l'émetteur du certificat CVC en utilisant la clé publique CA de CVC de laboratoire CTL détenue par l'élément de services PS;

4) valider la signature de l'émetteur de certificat CVC en utilisant la clé publique CA racine de certificat CVC de laboratoire CTL détenue par l'élément de services PS. La vérification de la signature authentifiera le certificat et confirmera la confiance dans la date de début de validité du certificat CVC;

5) mettre à jour la valeur actuelle des valeurs d'objet cvcAccessStart du titulaire avec la valeur de date de début de validité du certificat CVC. Si la valeur de date de début de validité est supérieure à la valeur actuelle de l'objet codeAccessStart de l'élément de services PS, mettre à jour la valeur de l'objet codeAccessStart de l'élément de services PS avec la valeur de début de validité.

11.3.7.7 Exigences de signature de code

11.3.7.7.1 Exigences d'autorité de certification (CA)

Les certificats de vérification de code (CVC) sont signés et produits par l'autorité CA de certificat CVC du laboratoire d'essais de certification (CTL). Le certificat CVC DOIT être exactement comme spécifié au § 11.3.7.3. L'autorité CA de CVC du laboratoire CTL NE DOIT PAS signer de certificat CVC à moins qu'il ne soit identique au format spécifié au § 11.3.7.3. Avant de signer un certificat CVC, l'autorité CA de CVC de laboratoire CTL DOIT vérifier que la demande de certificat est authentique.

L'autorité CA de CVC du laboratoire CTL sera responsable de l'enregistrement des noms des abonnés autorisés de certificat CVC. Les abonnés de certificat CVC incluent les constructeurs d'élément de services PS et les constructeurs et opérateurs qui vont cosigner les images de code. Il appartient à l'autorité CA de CVC du laboratoire CTL de garantir que le nom d'organisation de chaque abonné CVC est différent. Les directives suivantes DOIVENT être appliquées lors de l'attribution de noms d'organisation aux cosignataires de fichiers de code:

- le nom d'organisation utilisé pour s'identifier comme agent cosignataire de code dans un certificat CVC DOIT être attribué par l'organisation qui a produit le certificat racine;

- le nom DOIT être une chaîne imprimable de huit chiffres hexadécimaux qui distingue de façon non équivoque un agent signataire de code de tous les autres;
- chaque chiffre hexadécimal contenu dans le nom DOIT être choisi parmi l'ensemble de caractères 0-9 (0x30-0x39) ou A-F (0x41-0x46);
- la chaîne consistant en huit chiffres 0 n'est pas admise et NE DOIT PAS être utilisée dans un certificat CVC.

Dans tout format en variante, toutes les informations DOIVENT ETRE conservées et le format d'origine DOIT être reproduit, par exemple comme un entier de 32 bits différent de zéro avec une valeur d'entier égale à 0 représentant l'absence de signataire de code.

11.3.7.7.1.1 Exigences relatives au certificat CVC de constructeur

Pour signer leurs fichiers de code, les constructeurs DOIVENT obtenir un certificat CVC valide de l'autorité CA de CVC du laboratoire CTL. Toutes les images de code de constructeur fournies à un opérateur pour la mise à jour à distance d'un dispositif DOIVENT être signées conformément aux exigences définies dans la présente Recommandation. Lorsqu'il signe un fichier de code, un constructeur PEUT choisir de ne pas mettre à jour la valeur de l'objet signingTime de clé PKCS#7 dans les informations de signature du constructeur. La présente Recommandation exige que cete valeur soit égale ou supérieure à la date de début de validité du certificat CVC. Si le constructeur utilise une valeur d'objet signingTime égale à la date de début de validité du certificat CVC lorsqu'il signe une série de fichiers de code, ces fichiers de code peuvent être utilisés et réutilisés. Cela permet à un opérateur d'utiliser le fichier de code afin de surclasser ou de sous-classer la version de code pour les dispositifs de ce constructeur. Ces fichiers de code seront valides jusqu'à ce qu'un nouveau certificat CVC soit produit et reçu par l'élément de services PS.

11.3.7.7.1.2 Exigences relatives à l'opérateur

Lorsqu'un opérateur reçoit des fichiers de code de mise à jour logicielle de la part d'un constructeur, cet opérateur devrait valider l'image de code en utilisant la clé publique CA de certificat CV du laboratoire CTL. Cela permettra à l'opérateur de vérifier que l'image de code est telle qu'elle a été construite par le constructeur habilité. L'opérateur peut revérifier le fichier de code à tout moment en répétant le processus.

Si un opérateur veut exercer l'option de cosignature de l'image de code destinée à un dispositif de son réseau, cet opérateur DOIT obtenir un certificat CVC valide de l'autorité CA de CVC du laboratoire CTL.

Lorsqu'il signe un fichier de code, l'opérateur DOIT cosigner le contenu du fichier conformément à la norme de signature PKCS#7, et inclure son certificat CVC d'opérateur comme défini au § 11.3.7.2.1.1. La présente Recommandation n'exige pas d'un opérateur qu'il cosigne les fichiers de code mais, lorsque l'opérateur suit toutes les règles définies dans la présente Recommandation pour la préparation d'un fichier de code, l'élément de services PS DOIT l'accepter.

11.3.7.8 Processus de déclenchement

Les téléchargements de code, sans considération du mode d'approvisionnement, peuvent être initialisés pendant le processus d'approvisionnement et d'enregistrement via un téléchargement initialisé par le fichier de configuration, ou pendant le fonctionnement normal via la commande de téléchargement initialisée par le protocole SNMP. L'élément de services PS DOIT accepter les deux méthodes.

NOTE – Avant de déclencher un téléchargement sécurisé de logiciel, les informations appropriées de certificat CVC DOIVENT être incluses dans le fichier de configuration. Si l'opérateur décide d'utiliser le téléchargement initialisé par le protocole SNMP comme méthode pour déclencher un téléchargement sécurisé de logiciel, il est recommandé que les informations de certificat CVC soient toujours présentes dans le fichier de configuration, de façon que l'élément de services PS ait toujours les informations de CVC initialisées lorsqu'il en a besoin. Si l'opérateur décide d'utiliser le téléchargement initialisé par le fichier de

configuration PS comme méthode de déclenchement du téléchargement sécurisé de logiciel, les informations de CVC doivent nécessairement être présentes dans le fichier de configuration PS au moment où le dispositif est réamorcé pour obtenir le fichier de configuration PS qui déclenchera la mise à jour.

11.3.7.8.1 Téléchargement de logiciel initialisé par le protocole SNMP

A partir d'une station de gestion de réseau:

- mettre docsDevSwServer à l'adresse du serveur TFTP de mises à jour logicielles;
- mettre docsDevSwFilename au nom de chemin de fichier de l'image de mise à jour logicielle;
- mettre docsDevSwAdminStatus à Upgrade-from-mgt (*mise à jour venant de la gestion*). L'état de l'objet docsDevSwAdminStatus DOIT persister au-delà des réinitialisations/réamorçages jusqu'à ce qu'il soit modifié par un gestionnaire SNMP ou via le fichier de configuration PS de l'élément de services PS.

L'état par défaut de l'objet docsDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2} jusqu'à ce qu'il soit écrasé par la valeur ignoreProvisioningUpgrade{3} à la suite d'une mise à jour réussie de logiciel initialisée par le protocole SNMP ou autrement modifié par la station de gestion. L'état de l'objet docsDevSwOperStatus DOIT persister au-delà des réinitialisations afin de rapporter le résultat de la dernière tentative de mise à jour logicielle.

Si un élément de service subit une perte d'alimentation ou une réinitialisation pendant une mise à jour initialisée par le protocole SNMP, l'élément de services PS DOIT arrêter la mise à jour sans exiger d'intervention manuelle et, lorsque l'élément de services PS arrête le processus de mise à jour:

- docsDevSwAdminStatus DOIT être à la valeur Upgrade-from-mgt{1};
- docsDevSwFilename DOIT être le nom de fichier de l'image logicielle à mettre à jour;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant l'image mise à jour du logiciel à mettre à jour;
- docsDevSwOperStatus DOIT être à la valeur inProgress{1};
- docsDevSwCurrentVers DOIT être la version actuelle du logiciel qui fonctionne dans le dispositif.

Si l'élément de services PS atteint le nombre maximal de réessais (maximum de réessais = 3) à la suite de multiples pertes d'alimentation ou de réinitialisations pendant une mise à jour initialisée par le protocole SNMP, l'état de l'élément de services PS DOIT adhérer aux exigences suivantes après avoir été enregistré:

- docsDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2};
- docsDevSwFilename DOIT être le nom de fichier qui a échoué au processus de mise à jour;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué au processus de mise à jour;
- docsDevSwOperStatus DOIT être à la valeur other{5};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui fonctionne dans le dispositif IPCable2Home.

Si un élément de services PS épuise le nombre exigé de réessais TFTP en effectuant un total de 16 essais consécutifs, l'élément de services PS DOIT se replier sur la dernière image connue qui fonctionnait et se replier sur l'état opérationnel tout en suivant les exigences suivantes:

- docDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2};

- docDevSwFilename DOIT être le nom de fichier du logiciel qui a échoué au processus de mise à jour;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué au processus de mise à jour;
- docsDevSwOperStatus DOIT être à la valeur failed{4};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui fonctionne dans le dispositif.

Après que l'élément de services PS a terminé le téléchargement sécurisé de logiciel initialisé par le protocole SNMP, l'élément de services PS DOIT réamorcer et devenir opérationnel avec l'image correcte du logiciel et, une fois que le dispositif est opérationnel, il DOIT suivre les exigences suivantes:

- mettre son objet docsDevSwAdminStatus à la valeur ignoreProvisioningUpgrade{3};
- mettre son objet docsDevSwOperStatus à la valeur completeFromMgt{3};
- réamorcer.

L'élément de services PS DOIT utiliser de façon appropriée la valeur ignoreProvisioningUpgrade afin d'ignorer la valeur de mise à jour logicielle qui peut être incluse dans le fichier de configuration PS de l'élément de services PS et devenir opérationnel avec l'image logicielle correcte. Après que le dispositif est entré en fonctionnement, il DOIT adhérer aux exigences suivantes:

- docsDevSwAdminStatus DOIT être à la valeur ignoreProvisioningUpgrade{3};
- docsDevSwFilename PEUT être le nom de fichier du logiciel fonctionnant dans l'élément de services PS;
- docsDevSwServer PEUT être l'adresse du serveur TFTP contenant le logiciel qui fonctionne actuellement dans l'élément de services PS;
- docsDevSwOperStatus DOIT être à la valeur completeFromMgt{3};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui fonctionne dans l'élément de services PS.

Si l'élément de services PS réussit à télécharger (ou à détecter pendant le téléchargement) une image qui n'est pas destinée au dispositif, le:

- docsDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2};
- docsDevSwFilename DOIT être le nom de fichier du logiciel qui a échoué à la mise à jour;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué au processus de mise à jour;
- docsDevSwOperStatus DOIT être à la valeur other{5};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui fonctionne dans le dispositif.

Si l'élément de services PS détermine que l'image téléchargée a subi des dommages ou des corruptions, l'élément de services PS DOIT rejeter l'image nouvellement téléchargée. L'élément de services PS PEUT réessayer de télécharger si le nombre MAX de la séquence d'essais TFTP n'a pas été atteint. Si l'élément de services PS choisit de ne pas réessayer et que le nombre MAX de la séquence d'essais TFTP n'ait pas été atteint, l'élément de services PS DOIT se replier sur la dernière image connue qui fonctionnait, passer à un état opérationnel, générer les notifications d'événement appropriées comme spécifié au § 11.3.7.10, et adhérer aux exigences suivantes:

- docsDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2};
- docsDevSwFilename DOIT être le nom de fichier du logiciel qui a échoué à la mise à jour;

- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué à la mise à jour;
- docsDevSwOperStatus DOIT être à la valeur other{5};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui fonctionne dans le dispositif.

Si l'élément de services PS détermine que l'image est endommagée ou corrompue, l'élément de services PS DOIT rejeter l'image nouvellement téléchargée. L'élément de services PS PEUT tenter de télécharger une nouvelle image si le nombre MAX d'essais de séquence TFTP n'a pas été atteint. A la 16^{e} tentative de téléchargement de logiciel consécutive qui échoue, l'élément de services PS DOIT se replier sur la dernière image connue qui fonctionnait et passer à un état opérationnel. Dans ce cas, il est demandé à l'élément de services PS d'envoyer deux notifications, une pour signaler que la limite d'essais TFTP MAX a été atteinte, l'autre pour signaler que l'image est endommagée. Immédiatement après que l'élément de services PS a atteint l'état opérationnel, l'élément de services PS DOIT adhérer aux exigences suivantes:

- docsDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2};
- docsDevSwFilename DOIT être le nom de fichier du logiciel qui a échoué à la mise à jour;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué à la mise à jour;
- docsDevSwOperStatus DOIT être à la valeur other{5};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui fonctionne dans le dispositif.

11.3.7.8.2 Téléchargement de logiciel initialisé par le fichier de configuration

Le téléchargement de logiciel initialisé par le fichier de configuration PS est déclenché par l'envoi du nom de fichier de mise à jour logicielle contenu dans le fichier de configuration PS de l'élément de services PS. Si le nom de fichier de mise à jour logicielle contenu dans le fichier de configuration PS de l'élément de services PS ne correspond pas à l'image logicielle actuelle du dispositif, l'élément de services PS DOIT demander le fichier spécifié au serveur de logiciels via TFTP.

NOTE – L'adresse IP du serveur de logiciels est un paramètre distinct. S'il est présent, l'élément de services PS DOIT essayer de télécharger le fichier spécifié à partir de ce serveur. S'il n'est pas présent, l'élément de services PS DOIT essayer de télécharger le fichier spécifié à partir du serveur de fichiers de configuration.

Si l'élément de services PS atteint le nombre maximal d'essais (maximum d'essais = 3) résultant de pertes d'alimentation ou de réinitialisations multiples pendant une mise à jour initialisé par le fichier de configuration, l'état de l'élément de services PS DOIT adhérer aux exigences suivantes après son enregistrement:

- docsDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2};
- docsDevSwFilename DOIT être le nom de fichier du logiciel qui a échoué à la mise à jour;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué à la mise à jour;
- docsDevSwOperStatus DOIT être à la valeur other{5};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui fonctionne dans le dispositif.

Si un élément de services PS dépasse le nombre d'essais TFTP requis en produisant un total de 16 essais consécutifs, l'élément de services PS DOIT se replier sur la dernière image connue qui fonctionnait, passer à un état opérationnel, et adhérer aux exigences suivantes:

- docDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2};

- docDevSwFilename DOIT être le nom de fichier du logiciel qui a échoué au processus de mise à jour;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué au processus de mise à jour;
- docsDevSwOperStatus DOIT être à la valeur failed{4};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui fonctionne dans le dispositif.

Après que l'élément de services PS a terminé le téléchargement de logiciel initialisé par le fichier de configuration, l'élément de services PS DOIT réamorcer et devenir opérationnel avec l'image logicielle correcte. Après que l'élément de services PS est enregistré:

- docsDevSwAdminStatus DOIT être à la valeur allowProvisioningUpgrade{2};
- docsDevSwFilename PEUT être le nom de fichier du logiciel fonctionnant actuellement sur le dispositif IPCable2Home;
- docsDevSwServer PEUT être l'adresse du serveur TFTP contenant le logiciel fonctionnant actuellement sur le dispositif IPCable2Home;
- docsDevSwOperStatus DOIT être à la valeur completeFromProvisioning{2};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel fonctionnant dans le dispositif.

11.3.7.9 Vérification de code

Pour un téléchargement sécurisé de logiciel, l'élément de services PS DOIT effectuer les essais de vérification présentés dans le présent paragraphe. Si l'un des essais de vérification échoue, ou si une portion quelconque du fichier de code est rejetée à cause d'un format non valide, l'élément de services PS DOIT immédiatement arrêter le processus de téléchargement, enregistrer l'erreur s'il y a lieu, retirer tous les résidus du processus jusqu'à cette étape et continuer de fonctionner avec son code existant. Les essais de vérification peuvent être effectués dans n'importe quel ordre, pourvu que tous les essais applicables présentés dans ce paragraphe soient effectués.

1) L'élément de services PS DOIT valider les informations de signature du constructeur en vérifiant que la valeur signingTime (*date de signature*) de PKCS#7 est:
   a) égale ou supérieure à la valeur de l'objet codeAccessStart du constructeur actuellement détenue dans l'élément de services PS;
   b) égale ou supérieure à la valeur de date de début de validité du certificat CVC du constructeur;
   c) inférieure ou égale à la date de fin de validité du certificat CVC du constructeur.
2) L'élément de services PS DOIT valider le certificat CVC du constructeur en vérifiant que:
   a) le nom d'organisation titulaire du CVC est identique au nom de constructeur actuellement mémorisé par l'élément de services PS;
   b) la date de début de validité de certificat CVC est égale ou supérieure à la valeur cvcAccessStart du constructeur actuellement contenue dans l'élément de services PS;
   c) l'extension d'utilisation de clé étendue est exprimée en le certificat CVC comme défini au § 11.3.2.2.2.
3) L'élément de services PS DOIT valider la signature du certificat en utilisant la clé publique CA de CVC du laboratoire CTL détenue par l'élément de services PS. A son tour, la signature du certificat CA de CVC du laboratoire CTL est validée par la clé publique CA racine de CVC du laboratoire CTL détenue par l'élément de services PS. La vérification de la signature authentifiera la source de la clé de vérification de code (CVK, *code verification key*) publique et confirmera que la clé est fiable.

4) L'élément de services PS DOIT vérifier la signature du fichier de code du constructeur.

   a) L'élément de services PS DOIT effectuer un nouveau hachage SHA-1 sur le contenu SignedContent. Si la valeur du condensé de message ne correspond pas au nouveau hachage, l'élément de services PS DOIT considérer la signature sur le fichier de code comme non valide.

   b) Si la signature n'est pas vérifiée, tous les composants du fichier de code (y compris l'image de code), et toutes valeurs déduites du processus de vérification DOIVENT être rejetés et DEVRAIENT être immédiatement ignorés.

5) Si la signature du constructeur est vérifiée et que la signature d'un agent cosignataire soit requise:

   a) l'élément de services PS DOIT valider les informations de signature du cosignataire en vérifiant que:

      i) les informations de signature du cosignataire sont incluses dans le fichier de code;

      ii) la valeur signingTime de PKCS#7 est égale ou supérieure à la valeur correspondante de l'objet codeAccessStart actuellement contenue dans l'élément de services PS;

      iii) la valeur PKCS#7 de signingTime est égale ou supérieure à celle de la date de début de validité de CVC correspondante;

      iv) la valeur signingTime de PKCS#7 est inférieure ou égale à la date de fin de validité du certificat CVC correspondant;

   b) l'élément de services PS DOIT valider le certificat CVC du cosignataire en vérifiant que:

      i) le nom d'organisation titulaire du certificat CVC est identique au nom d'organisation du cosignataire actuellement mémorisé par l'élément de services PS;

      ii) la date de début de validité du certificat CVC est égale ou supérieure à la valeur cvcAccessStart actuellement contenue dans l'élément de services PS pour le nom d'organisation titulaire correspondant;

      iii) l'extension d'usage de clé étendue est exprimée en le certificat CVC comme défini au § 11.3.2.2.2;

   c) l'élément de services PS DOIT valider la signature du certificat en utilisant la clé publique CA de CVC du laboratoire CTL détenue par l'élément de services PS. A son tour, la signature de certificat CA de CVC du laboratoire CTL est validée par la clé publique CA racine de CVC contenue dans l'élément de services PS. La vérification de la signature va authentifier la source de la clé de vérification de code (CVK) du cosignataire et confirmer que la clé est fiable;

   d) l'élément de services PS DOIT vérifier la signature de fichier de code du cosignataire;

   e) l'élément de services PS DOIT effectuer un nouveau hachage SHA-1 sur le contenu SignedContent. Si la valeur du condensé de message ne correspond pas au nouveau hachage, l'élément de services PS DOIT considérer que la signature sur le fichier de code est invalide;

   f) si la signature n'est pas vérifiée, tous les composants du fichier de code (y compris l'image de code) et toutes les valeurs déduites du processus de vérification DOIVENT être rejetés et DEVRAIENT être immédiatement ignorés.

6) Si la signature du constructeur, et facultativement du cosignataire, est vérifiée, l'image de code peut être considérée comme fiable et l'installation peut se poursuivre. Avant d'installer l'image de code, tous les autres composants du fichier de code et toutes les valeurs déduites

du processus de vérification à l'exception des valeurs de signingTime PKCS#7 et de début de validité du certificat CVC DEVRAIENT être immédiatement supprimés.

7) Si l'installation de code échoue, l'élément de services PS DOIT rejeter les valeurs de signingTime PKCS#7 et de début de validité du certificat CVC qu'il vient de recevoir dans le fichier de code.

8) Lorsque l'installation de code est réussie, l'élément de services PS DOIT mettre à jour les commandes du constructeur qui sont dépendantes du temps avec les valeurs provenant des informations de signature et du certificat CVC du constructeur:

   a) mettre à jour la valeur actuelle de l'objet codeAccessStart avec la valeur signingTime PKCS#7;

   b) mettre à jour la valeur actuelle de l'objet cvcAccessStart avec la valeur de début de validité de certificat CVC.

9) Lorsque l'installation de code est réussie, SI le fichier de code était cosigné, l'élément de services PS DOIT mettre à jour les commandes du cosignataire qui varient selon le temps avec les valeurs provenant des informations de signature et du CVC du cosignataire:

   a) mettre à jour la valeur actuelle de l'objet codeAccessStart avec la valeur signingTime PKCS#7;

   b) mettre à jour la valeur actuelle de l'objet cvcAccessStart avec la valeur de début de validité de certificat CVC.

11.3.7.10 Codes d'erreur

Des codes d'erreur sont définis afin d'indiquer les états d'échec possibles pendant le processus de vérification de code de téléchargement de logiciel sécurisé.

1) commandes de fichier de code inappropriées:

   a) le nom d'organisation titulaire de CVC pour le constructeur ne correspond pas au nom de constructeur de l'élément de services PS;

   b) le nom d'organisation titulaire de CVC pour l'agent cosignataire ne correspond pas à l'agent cosignataire de code actuel de l'élément de services PS;

   c) la valeur signingTime PKCS#7 est inférieure à la valeur de l'objet codeAccessStart actuellement contenue dans l'élément de services PS;

   d) la valeur de date de début de validité PKCS#7 du constructeur est inférieure à la valeur de l'objet cvcAccessStart actuellement contenue dans l'élément de services PS;

   e) la date de début de validité du certificat CVC du constructeur est inférieure à la valeur de l'objet cvcAccessStart actuellement contenue dans l'élément de services PS;

   f) la valeur signingTime PKCS#7 du constructeur est inférieure à la date de début de validité du certificat CVC;

   g) l'extension d'usage de clé étendu manque ou est inappropriée dans le certificat CVC du constructeur;

   h) la valeur signingTime PKCS#7 du cosignataire est inférieure à la valeur de l'objet codeAccessStart actuellement contenue dans l'élément de services PS;

   i) la valeur de date de début de validité PKCS#7 du cosignataire est inférieure à la valeur de l'objet cvcAccessStart actuellement contenue dans l'élément de services PS;

   j) la date de début de validité du certificat CVC du cosignataire est inférieure à la valeur de l'objet cvcAccessStart actuellement contenue dans l'élément de services PS;

   k) la valeur signingTime PKCS#7 du cosignataire est inférieure à la date de début de validité du certificat CVC;

l) l'extension d'usage de clé étendu manque ou est inappropriée dans le certificat CVC du cosignataire.

2) échec de la validation du certificat CVC du constructeur du fichier de code;

3) échec de la validation de la signature CVS du constructeur du fichier de code;

4) échec de la validation du certificat CVC du cosignataire du fichier de code;

5) échec de la validation de la signature CVS du cosignataire du fichier de code;

6) format de certificat CVC de fichier de configuration inapproprié (par exemple, attribut d'usage de clé manquant ou impropre);

7) échec de la validation du certificat CVC du fichier de configuration;

8) format du certificat CVC de protocole SNMP inapproprié:

   a) le nom d'organisation titulaire de certificat CVC pour le constructeur ne correspond pas au nom de constructeur du dispositif;

   b) le nom d'organisation titulaire de certificat CVC pour l'agent cosignataire de code ne correspond pas à l'agent cosignataire de code actuel de l'élément de services PS;

   c) la date de début de validité du certificat CVC est inférieure ou égale à la valeur de l'objet cvcAccessStart du titulaire actuellement contenue dans l'élément de services PS;

   d) Attribut d'usage de clé manquant ou impropre;

9) échec de la validation du certificat CVC de protocole SNMP.

11.3.7.11 Repli du logiciel

Le repli du logiciel définit le processus de retrait de la version mise à jour du téléchargement de l'image logicielle, et donc du retour du dispositif à l'exact état antérieur.

Lorsque l'élément de services PS reçoit un fichier de code avec une date de signature postérieure à celle de la valeur mémorisée, le dispositif DOIT actualiser sa mémoire interne avec la valeur reçue.

Comme l'élément PS n'acceptera pas de fichiers de code avec une date de signature antérieure à celle de la valeur mémorisée, le signataire peut choisir de ne pas mettre à jour la date de signature lorsqu'il met à jour un dispositif avec un nouveau fichier de code et qu'il veut éviter d'interdire l'accès aux anciens fichiers de code. De cette façon, de multiples fichiers de code ayant la même date de signature de code permettent à un opérateur de replier librement une image de code d'un dispositif sur une version ancienne (c'est-à-dire jusqu'à ce que le certificat CVC soit mis à jour). Cela présente un certain nombre d'avantages pour l'opérateur, mais ces avantages devraient être soigneusement pesés au regard des risques d'attaque par répétition du fichier de code.

Une autre approche consisterait à signer le fichier de code précédent avec une date de signature égale ou supérieure à la date de signature de la dernière mise à jour.

11.3.8 Sécurité physique

La présente Recommandation exige que le service portail assure la maintenance, dans sa mémoire, des clés et autres variables cryptographiques se rapportant à la sécurité du réseau. Tous les éléments et dispositifs DOIVENT empêcher l'accès physique non autorisé à ce matériel cryptographique.

Le niveau de protection physique du matériau de clé exigé pour les éléments de réseau et dispositifs est spécifié en termes de niveaux de sécurité dans le document FIPS PUBS 140-2, Exigences de sécurité pour les modules cryptographiques. En particulier, les éléments IPCable2Home DOIVENT satisfaire les exigences du niveau 1 de sécurité de la norme FIPS PUBS 140-2.

Le niveau 1 de sécurité de la norme FIPS PUBS 140-2 exige une protection physique minimale par l'utilisation d'enceintes de qualité de production et de pratiques logicielles recommandées.

11.3.9 Algorithmes cryptographiques

11.3.9.1 SHA-1

L'implémentation de l'algorithme SHA-1 dans l'environnement IPCable2Home DOIT utiliser l'algorithme de hachage SHA-1 qui est défini dans le document FIPS 180-2.

12 Processus de gestion

12.1 Introduction/Aperçu général

Le présent paragraphe donne des exemples de traitements associés à l'utilisation des utilitaires décrits au § 6 (Utilitaires de gestion) et des traitements supplémentaires qui facilitent d'autres fonctions obligatoires de gestion définies dans la présente Recommandation. L'accès à la base de données des services PS et d'autres opérations des services PS du portail de gestion câble (CMP) sont décrites au § 6. Les règles types d'accès à une base MIB figurent au § 6.3.6.

Les processus relatifs à la gestion et d'autres processus descriptifs sont fournis pour les scénarios suivants:

- processus des utilitaires de gestion;
- fonctionnement du portail CTP:
  - utilitaire de vitesse de connexion;
  - utilitaire de validation par écho;
- fonctionnement des services PS;
- accès à la base de données des services PS;
- reconfiguration:
  - téléchargement de logiciel de services portail;
  - téléchargement de fichier de configuration PS;
- accès à la base MIB;
- configuration du modèle VACM;
- configuration de messagerie d'événements de gestion:
  - fonctionnement de la notification d'événement de portail CMP;
  - fonctionnement du ralentissement et de la limitation d'événements de portail CMP.

12.1.1 Objectifs

Le présent paragraphe est principalement composé d'un texte informatif qui est destiné à faciliter la compréhension par le lecteur et qui ne contient aucune exigence. Les exemples décrivent le mode d'utilisation des utilitaires de gestion pour l'accomplissement des fonctions de gestion typiques. Des organigrammes séquentiels des processus supplémentaires se rapportant à la gestion (c'est-à-dire, ceux qui ne sont pas définis au § 6) sont également fournis, y compris les processus de gestion ou les étapes des processus associés à l'utilisation des utilitaires de gestion obligatoires. Tous les processus indiqués impliquent l'interaction de l'élément de services PS avec les systèmes de tête de réseau.

12.2 Processus d'utilitaires de gestion

Les processus d'utilitaires de gestion sont ceux qui sont associés aux utilitaires de gestion obligatoires définis au § 6.

12.2.1 Fonctionnement du portail CTP

Le portail d'essai du câble (CTP) fournit des fonctions d'essai à distance de vitesse de connexion et d'essai de validation par écho, décrites respectivement au § 6.4.3.1 et au § 6.4.3.2.

12.2.1.1 Essai à distance de vitesse de connexion

L'essai à distance de vitesse de connexion peut servir à valider les niveaux de performance, identifier les erreurs possibles de configuration et déterminer d'autres caractéristiques visant les performances.

- Le système de gestion de réseau (NMS) commence l'essai en initialisant les paramètres d'essai et en activant le fanion de début d'essai, via la demande SET du protocole SNMP.
- L'agent SNMP de portail CMP met à jour la base de données de services portail avec les paramètres d'essai et notifie au portail CTP qu'il y a lieu de commencer l'essai.
- Le portail CTP interroge la base de données de services portail concernant les paramètres d'essai.
- Le portail CTP produit une rafale de paquets UDP vers le point d'accès 7 du dispositif IP de réseau LAN spécifié. Le point d'accès 7 est réservé au service d'écho.
- Le dispositif IP de réseau LAN cible renvoie simplement en écho au portail CTP la charge utile de paquet UDP.
- Une fois que tous les paquets ont été reçus, ou que la période de temporisation de l'essai est arrivée à expiration, le portail CTP met à jour la base de données du service portail avec les résultats de l'essai et active le fanion d'essai terminé.
- Le système NMS vérifie que la commande est terminée en vérifiant que la valeur de l'objet Status est "complete" (terminé).
- Le système NMS demande les résultats des essais via la demande GET du protocole SNMP.
- L'agent SNMP de portail CMP interroge la base de données du service portail concernant les résultats d'essai et en fait rapport dans la réponse GET du protocole SNMP. Si l'essai n'est pas terminé, les données de l'essai indiqueront que l'essai est toujours en cours. Le système NMS doit répéter la demande GET du protocole SNMP jusqu'à ce que les résultats de l'essai indiquent que l'essai est terminé.

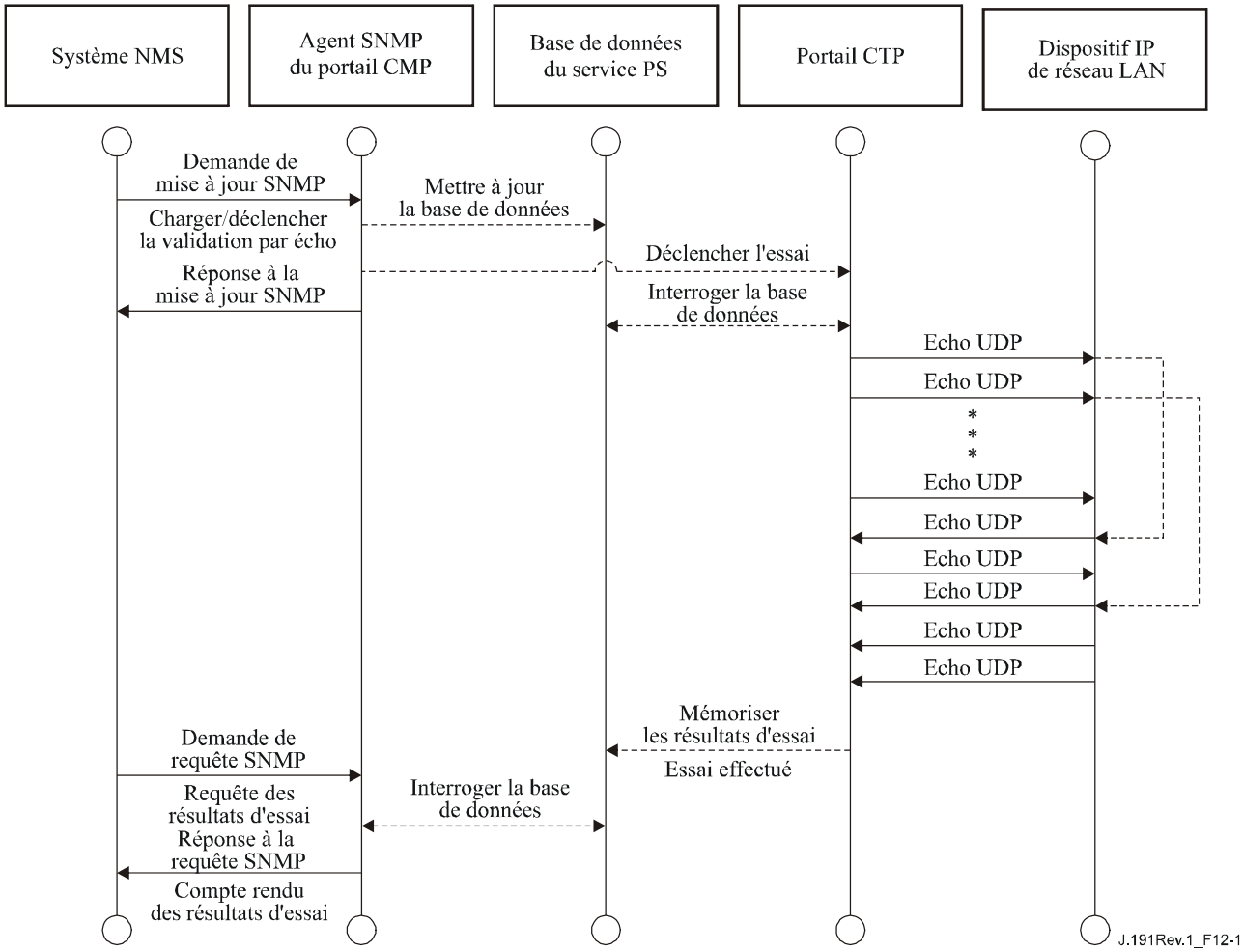


Figure 12-1/J.191 – Diagramme séquentiel d'essai de vitesse de connexion

12.2.1.2 Processus de validation par écho

L'essai de validation par écho peut servir à la validation de l'état de connexité, des niveaux de performance, et à identifier les erreurs de configuration possibles.

- Le système NMS commence l'essai en initialisant les paramètres d'essai et en activant le fanion de début d'essai, via la demande SET (mise à jour) du protocole SNMP.
- L'agent SNMP de portail CMP met à jour la base de données du service portail avec les paramètres d'essai et notifie au portail CTP qu'il y a lieu de commencer l'essai.
- Le portail CTP interroge la base de données du service portail concernant les paramètres d'essai.
- Le portail CTP envoie un paquet de demande d'écho ICMP au dispositif IP de réseau LAN spécifié.
- Le dispositif IP de réseau LAN cible renvoie une réponse d'écho ICMP.
- Le portail CTP met à jour la base de données du service portail avec les résultats de l'essai et active le fanion d'essai terminé.
- Le système NMS vérifie que la commande est exécutée en vérifiant que la valeur de l'objet Status est "complete" (terminé).
- Le système NMS demande les résultats de l'essai via la demande GET (requête) du protocole SNMP.

- L'agent SNMP du portail CMP interroge la base de données du service portail concernant les résultats de l'essai et en fait rapport dans la réponse GET du protocole SNMP. Si l'essai n'est pas terminé, les données d'essai indiqueront que l'essai est toujours en cours. Le système NMS doit répéter la demande GET du protocole SNMP jusqu'à ce que les résultats d'essai indiquent que l'essai est terminé.

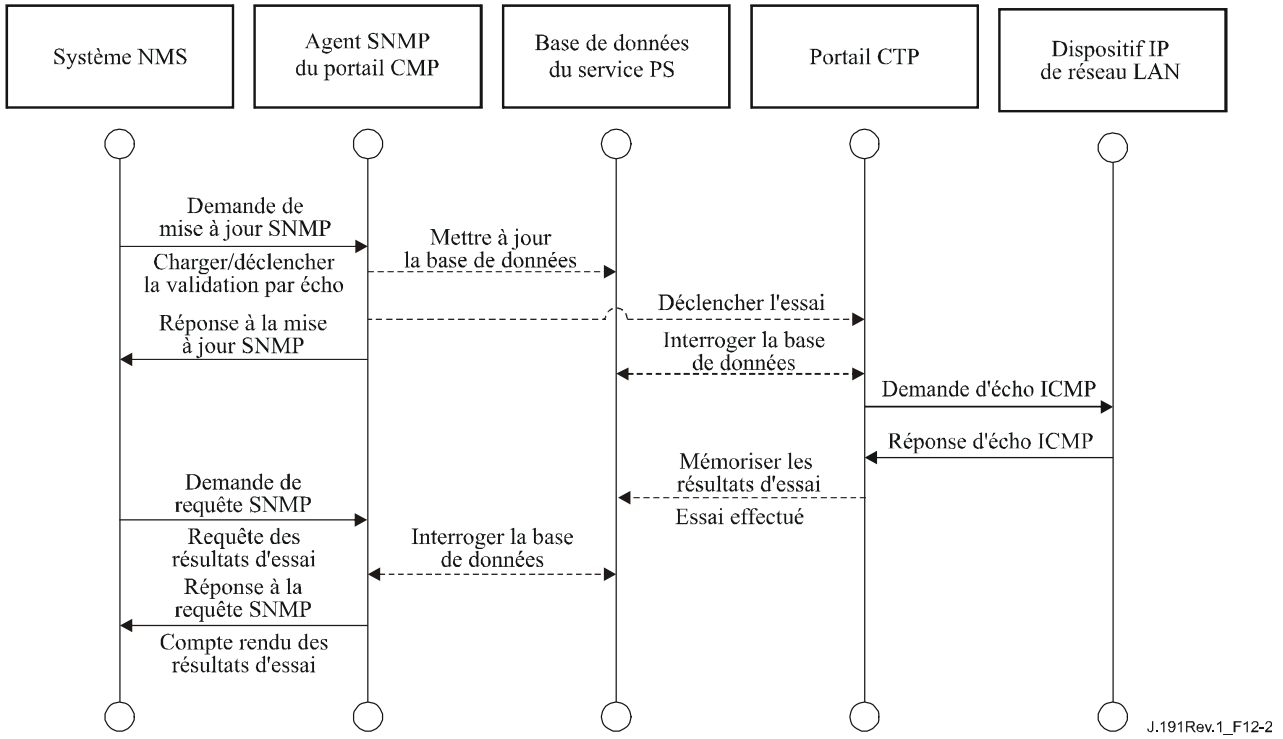


Figure 12-2/J.191 – Diagramme séquentiel d'essai de validation par écho

12.3 Fonctionnement du service portail

Le portail de gestion du câble (CMP) donne accès à la base de données du service portail via l'interface PS/réseau WAN-Man, comme décrit au § 6. La séquence de messages pour un fonctionnement à distance d'accès à une base de donnée de services portail à partir de l'interface PS/réseau WAN-Man est décrite ci-dessous.

12.3.1 Accès à une base de données de services portail

Le système NMS accède aux paramètres de configuration et de gestion mémorisés dans la base de données du service portail via les bases MIB du protocole SNMP. Les paramètres sont récupérés au moyen des messages Get-Request (demande de mise à jour), Get-Next-Request (demande de requête suivante), et Get-Bulk (requête générale) du protocole SNMP produits par le système NMS avec l'adresse WAN-Man du service portail comme adresse de destination. Des paramètres peuvent être modifiés et des actions (comme les essais de vitesse de connexion et de validation par écho) peuvent être exécutées par l'envoi de messages Set-Request (demande de mise à jour) du protocole SNMP avec les paramètres appropriés, à l'adresse WAN-Man du service portail, à l'initiative du système NMS.

La Figure 12-3 décrit les séquences de messages de gestion pour un accès de base de données de services portail typique, à partir d'une interface PS/réseau WAN-Man. Les séquences de messages supposent qu'une liaison SNMPv3 sécurisée a été établie.

- Le système NMS extrait les données de la base de données du service portail en utilisant la demande GET du protocole SNMP. Cette demande énumère les objets spécifiques que le système NMS cherche à extraire de la base de données.
- L'agent SNMP du portail CMP interroge la base de données du service portail concernant les paramètres spécifiés.
- L'agent SNMP du portail CMP rapporte les données au système NMS avec la réponse GET du protocole SNMP.

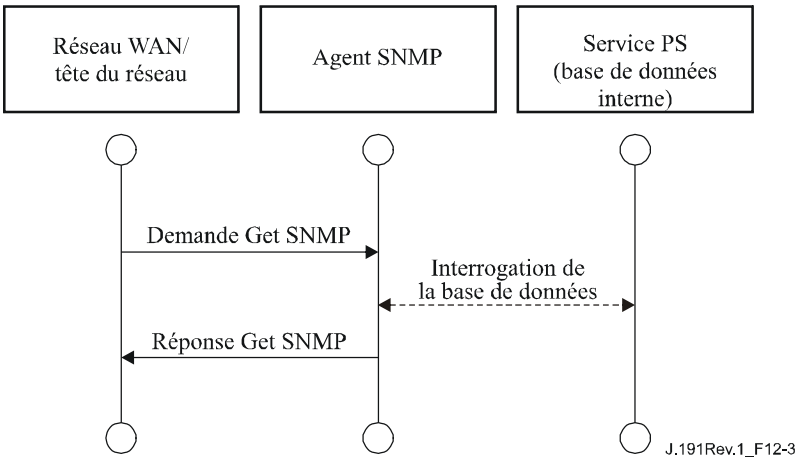


Figure 12-3/J.191 – Diagramme séquentiel de l'accès à la base de données du service portail à partir de l'interface entre ce service et le réseau WAN-Man

12.3.2 Reconfiguration

12.3.2.1 Téléchargement de logiciel de service portail

La Figure 12-4 illustre un processus de téléchargement de logiciel/micrologique pour un service portail en mode d'approvisionnement SNMP. Ce processus est déclenché par le système NMS. Le service portail est informé de l'adresse lui permettant d'obtenir le nouveau logiciel de fichier de code. Une fois le téléchargement du fichier de code achevé, le service portail va contrôler l'image pour chercher toute altération qui aurait pu survenir pendant le téléchargement. L'authentification est effectuée afin de vérifier que le fichier de code peut être considéré comme fiable. Après cette étape, un réamorçage du système est effectué.

Après ce réamorçage, le service portail reprend son fonctionnement avec la nouvelle image logicielle. Le service portail peut avoir besoin d'être reconfiguré après la mise à jour logicielle et les interfaces WAN peuvent avoir besoin d'être réapprovisionnées (ce qui n'est pas montré dans l'exemple). Si le service portail n'accepte pas la nouvelle image logicielle, il va revenir à la précédente version de logiciel (sauvegarde) et signaler au système NMS de ce qui est arrivé.

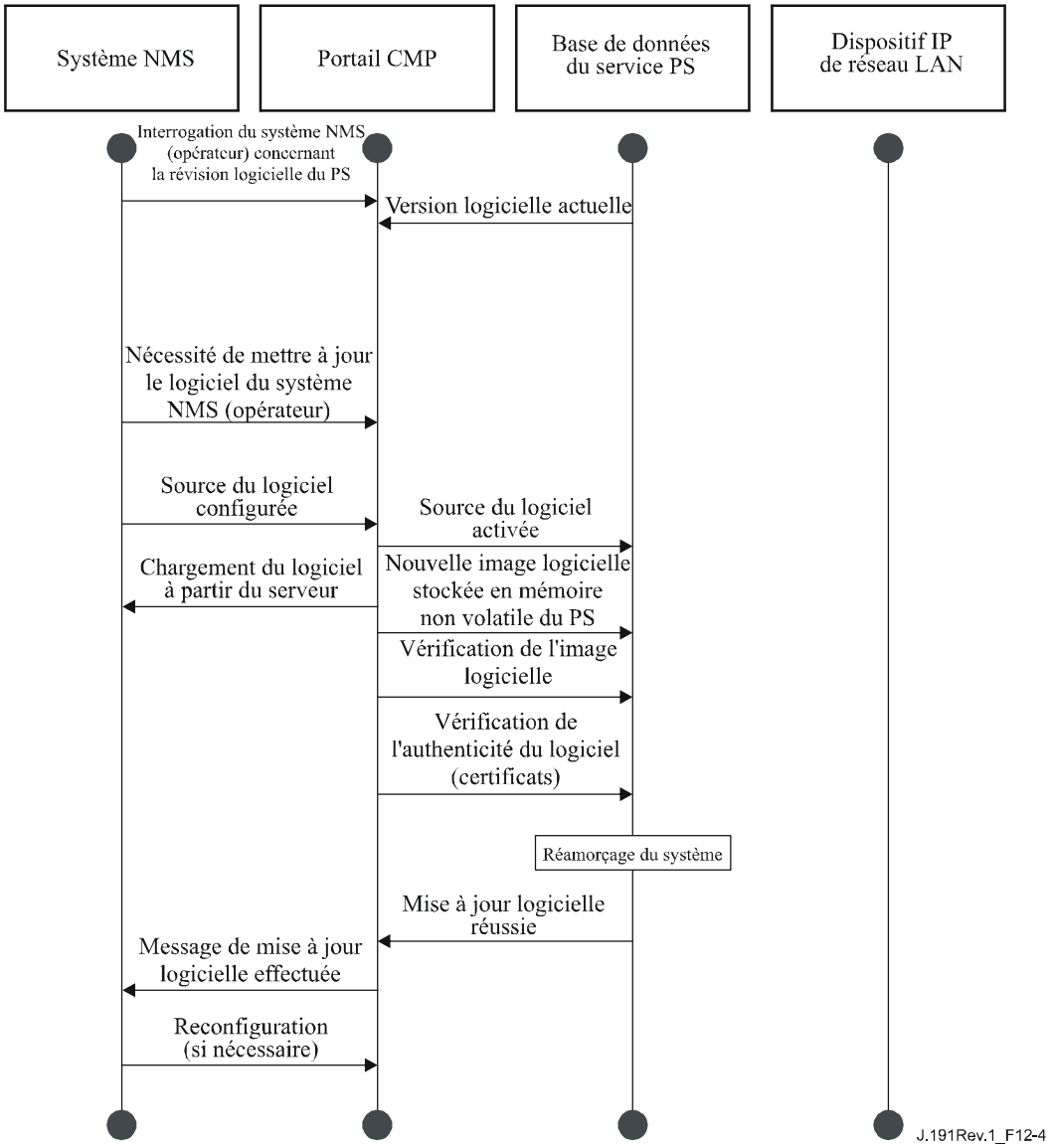


Figure 12-4/J.191 – Diagramme séquentiel de téléchargement de logiciel pour le service portail

12.3.2.2 Téléchargement de fichier de configuration PS pour le service portail

La Figure 12-5 illustre une reconfiguration d'un service PS en mode d'approvisionnement SNMP, via le téléchargement d'un fichier de configuration. Ce processus est déclenché par le système NMS. Le fichier de configuration PS est donné au service portail par inscription du serveur de fichier et du nom de fichier dans le service portail, et par déclenchement du téléchargement du fichier par le service portail. Une fois le fichier de configuration PS chargé, les commandes qui y sont contenues sont interprétées. Si l'une des commandes n'est pas comprise ou n'est pas applicable, elle est sautée et un événement est produit. Lorsque le service portail a terminé de traiter le fichier de configuration, il enregistre le nombre de nuplets de TLV traités et sautés dans les objets de base MIB appropriés.

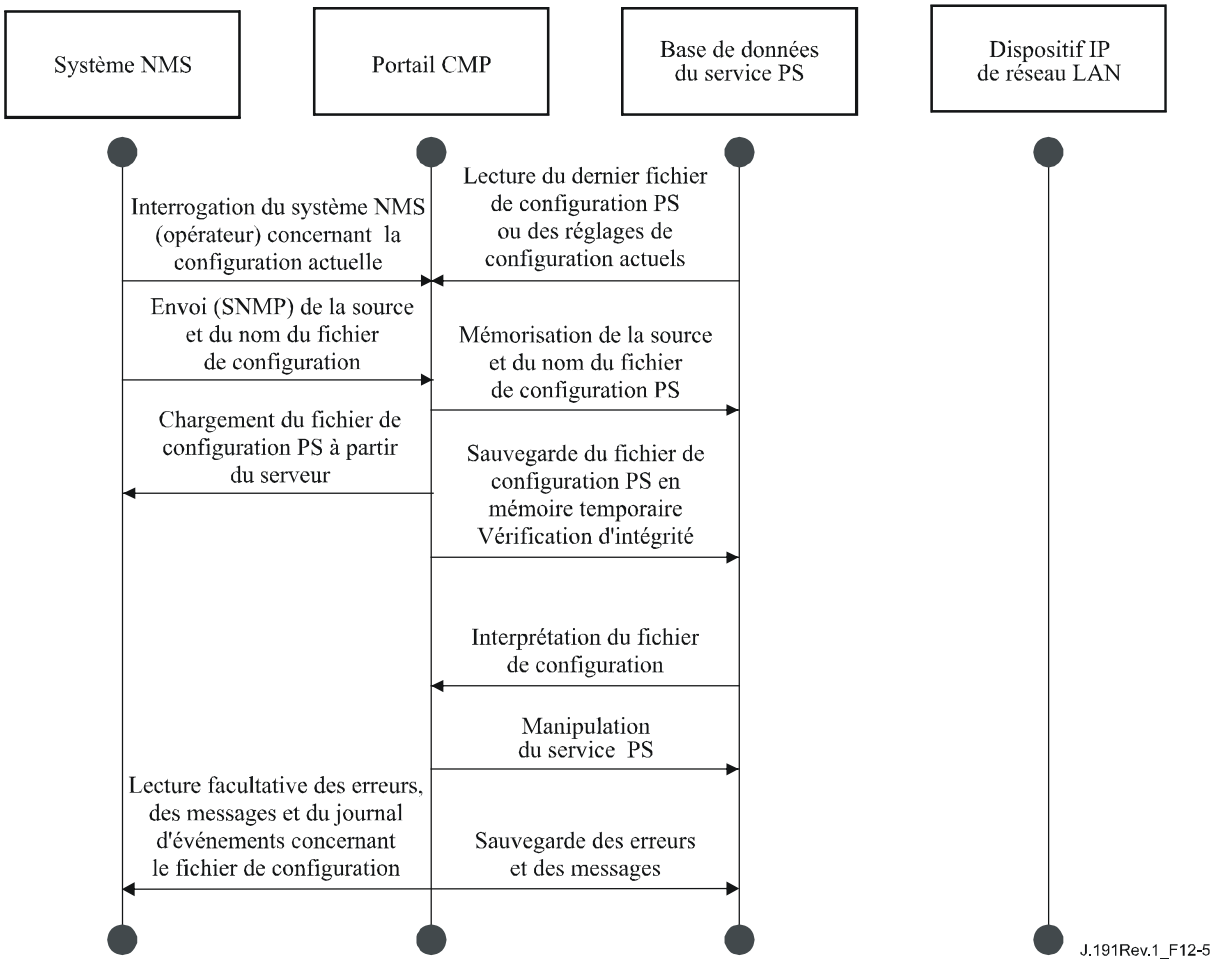


Figure 12-5/J.191 – Diagramme séquentiel de reconfiguration du service PS (téléchargement de fichier de configuration)

12.4 Accès de base MIB

12.4.1 Configuration du modèle VACM

Le câblo-opérateur a le contrôle du domaine de gestion. Un exemple de la configuration des paramètres du modèle VACM est montré dans la Figure 12-6.

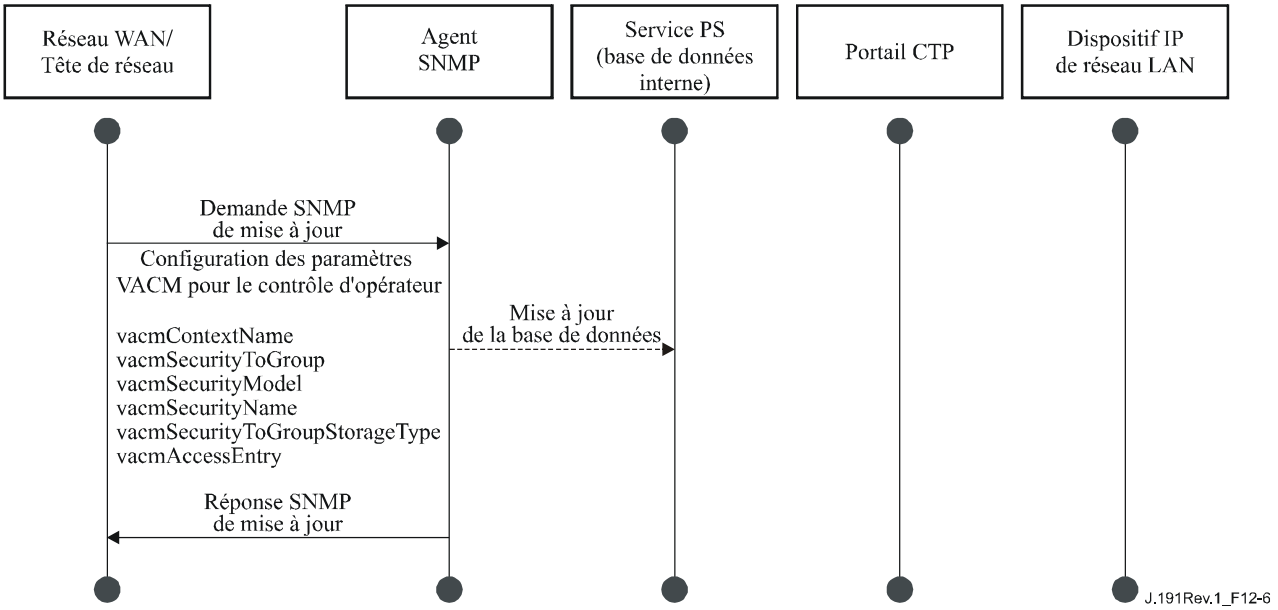


Figure 12-6/J.191 – Séquence de configuration du service PS (paramètres VACM)

12.4.2 Configuration de messagerie d'événement de gestion

12.4.2.1 Fonctionnement de la notification d'événement au portail CMP

Les événements sont rapportés au moyen d'enregistrements d'événements locaux, de messages SNMP TRAP, SNMP INFORM, et SYSLOG. Le mécanisme de notification d'événement peut être établi ou modifié par le système NMS, par production d'un message de demande SET du protocole SNMP à l'adresse WAN-Man du service portail.

La Figure 12-7 illustre la façon de configurer la base de données du service portail pour mémoriser les événements dans les fichiers d'enregistrement locaux. Les événements d'enregistrement local sont de deux types: local-non volatile et local-volatile. Le système NMS lira le contenu de l'enregistrement local et écrira ce contenu dans le système d'enregistrement d'événements de la tête de réseau. Un réamorçage du service portail ne provoque l'effacement que des événements volatiles de la base de données du service portail. Les événements non volatiles persistent d'un réamorçage à l'autre.

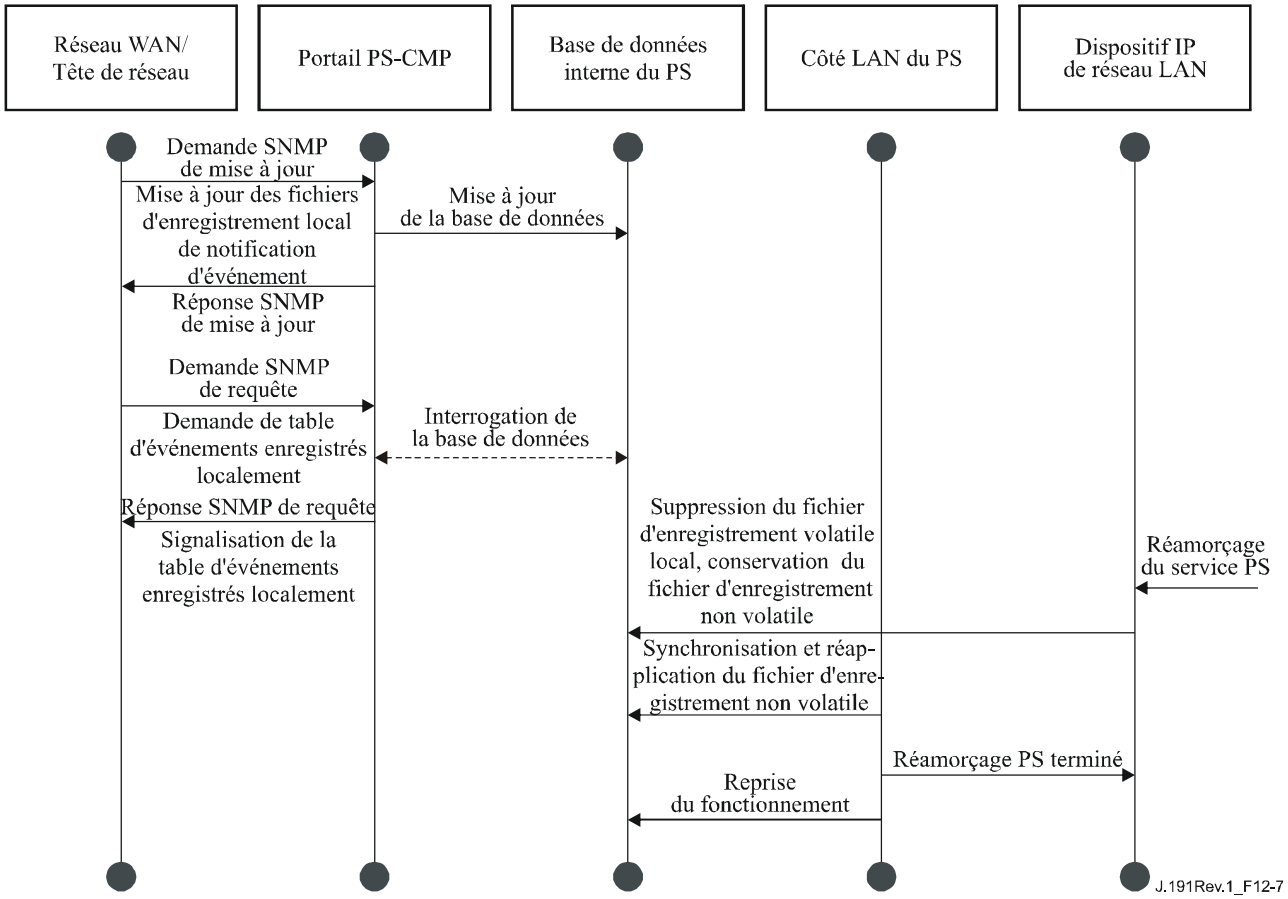


Figure 12-7/J.191 – Séquence de configuration du service PS (contrôle d'événement)

La Figure 12-8 illustre le téléchargement d'un fichier de configuration PS pour un service portail en mode d'approvisionnement SNMP. Ce processus est déclenché via une demande SET (mise à jour) du protocole SNMP. Le service portail doit vérifier ce fichier avant de l'accepter. Dans l'exemple, il existe une erreur de TLV dont il est fait rapport. Dans la mesure où la notification d'événement est mise au mode TRAP du protocole SNMP, l'adresse du serveur de messages TRAP est récupérée dans la base de données du service portail et l'événement est envoyé au serveur de messages TRAP.

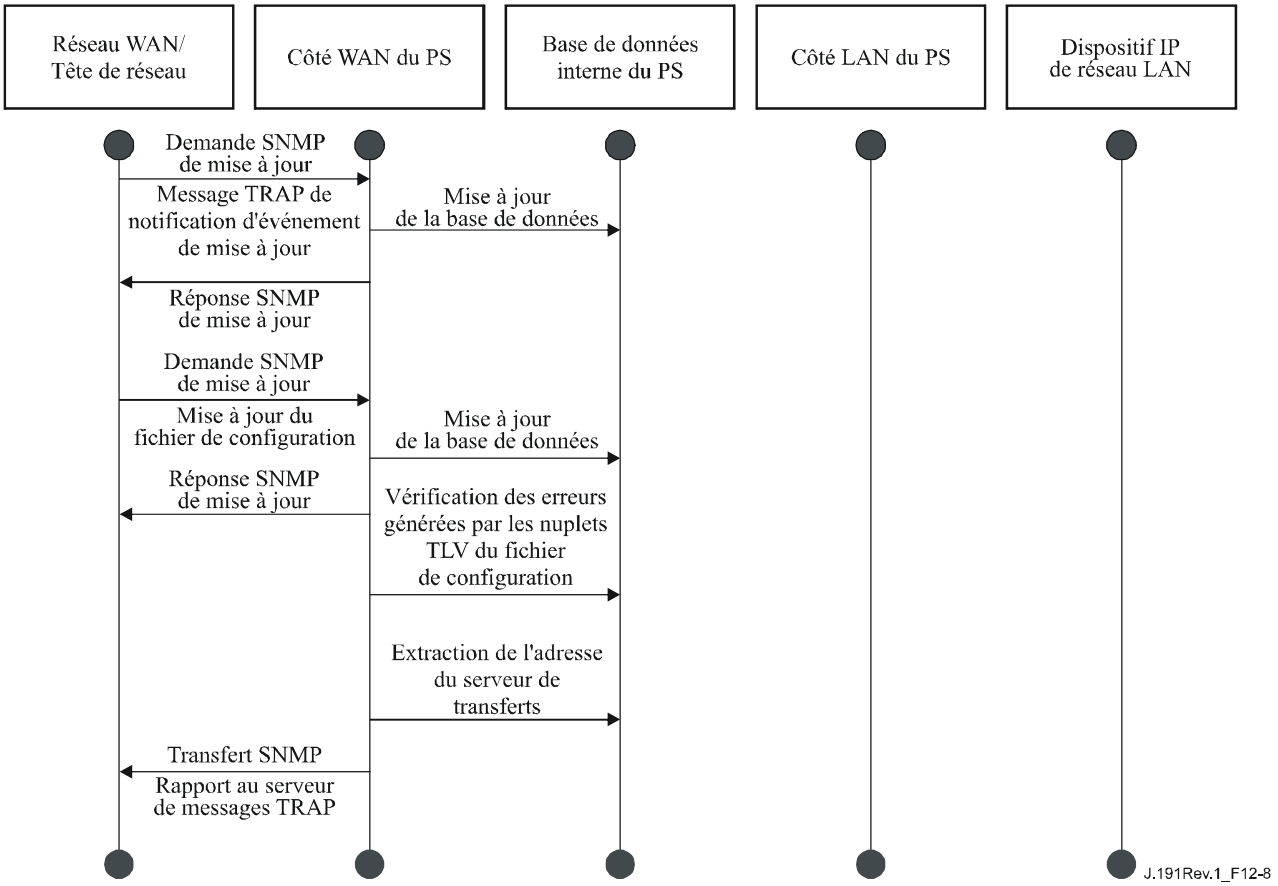


Figure 12-8/J.191 – Séquence de téléchargement de fichier de configuration PS de service portail (avec des nuplets TLV non valides)

La Figure 12-9 illustre le processus d'un dispositif IP de réseau LAN essayant d'obtenir une adresse IP du serveur DHCP (serveur CDS). La fonction de serveur CDS vérifie la base de données du service portail afin de trouver une adresse IP disponible. Dans ce cas, le serveur CDS détecte qu'il n'y a pas d'adresse IP disponible dans le groupe d'adressage et il envoie un événement au serveur SYSLOG.

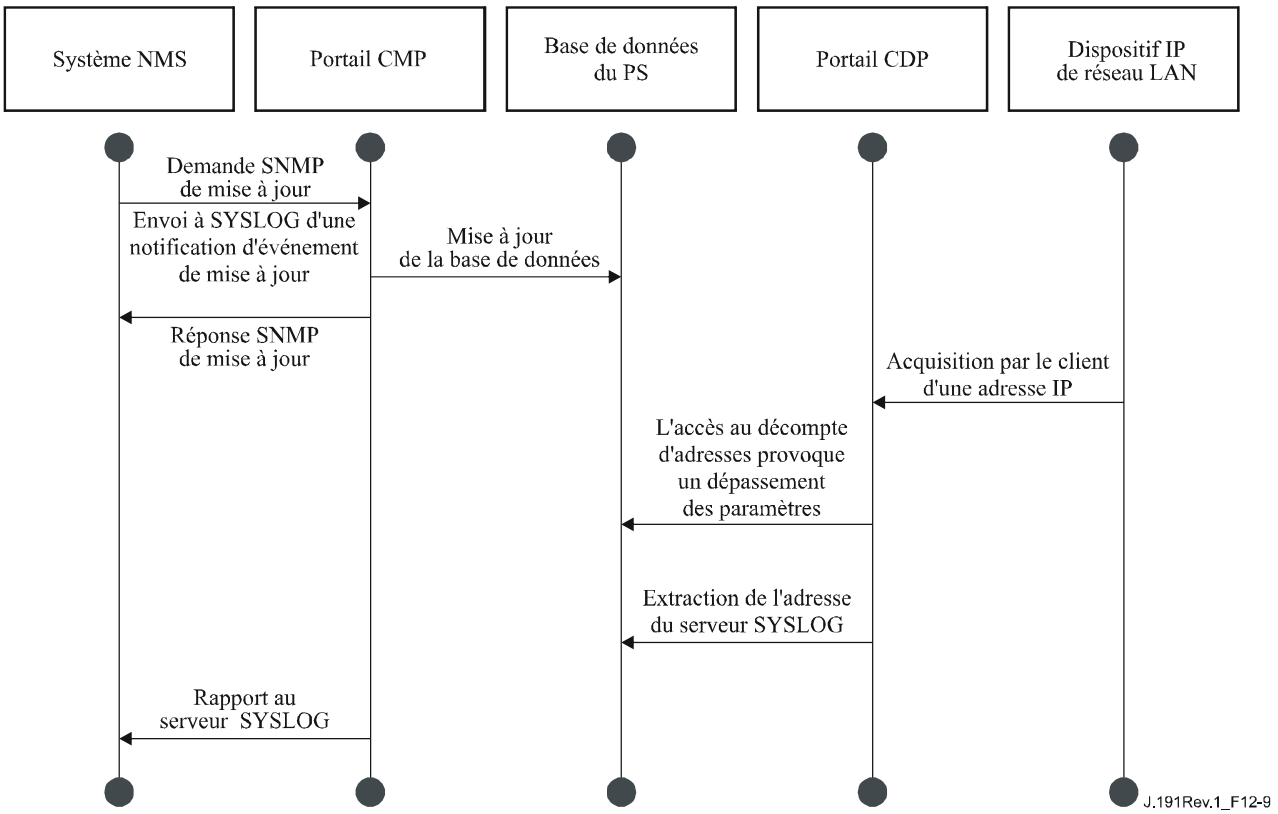


Figure 12-9/J.191 – Séquence d'acquisition d'adressede dispositif IP de réseau LAN (demande dépassant le compte approvisionné)

12.4.2.2 Exemple de fonctionnement de ralentissement et de limitation d'événements au portail CMP

Un mécanisme de ralentissement d'événements est fourni par la fonctionnalité de portail CMP du service PS. Le ralentissement et la limitation d'événements est très souple et peut inclure des cas dans lesquels les événements sont rapportés et des cas dans lesquels aucun événement n'est rapporté au système NMS. Voir au § 6.5.3 une description du mécanisme de ralentissement et de limitation d'événements au portail CMP.

La Figure 12-10 illustre la configuration de la base de données du service PS pour renvoyer des événements via la méthode INFORM du protocole SNMP. Au départ, plusieurs messages INFORM sont écrits dans le fichier d'enregistrement local et sont acheminés au système NMS. Le mécanisme de ralentissement d'événements fixe la limite du nombre d'événements qui peuvent être envoyés au système NMS dans un laps de temps donné. Lorsque cette limite est atteinte, le service portail arrête d'envoyer des messages INFORM au système NMS. Afin de relancer la notification d'événements, le système NMS devrait réactiver le rapport d'événements.

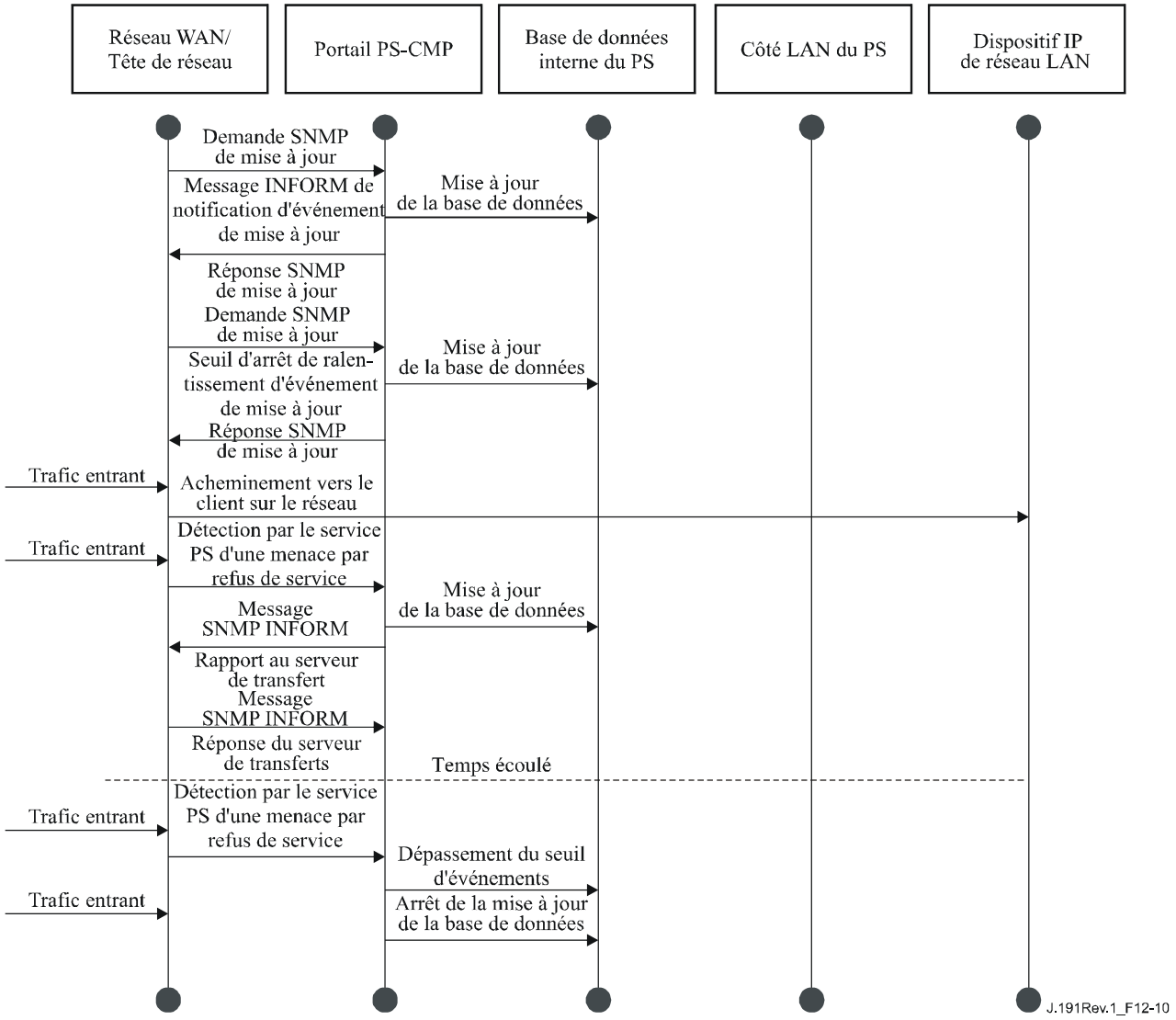


Figure 12-10/J.191 – Fonctionnement du ralentissement et de la limitation d'événements au portail CMP

13 Processus d'approvisionnement

Le présent paragraphe décrit les processus impliqués lors de l'utilisation des utilitaires d'approvisionnement décrits au § 7, pour l'approvisionnement initial du dispositif IP de réseau LAN et de l'élément de services PS. L'approvisionnement recouvre les trois tâches suivantes:

1) acquisition des adresses de réseau;

2) acquisition des informations de serveur;

3) téléchargement sécurisé et traitement du fichier de configuration PS.

Les processus d'approvisionnement sont décrits dans le présent paragraphe pour chacun des cas pertinents suivants:

- WAN-Man de services portail – Approvisionnement de la fonctionnalité de gestion fondée sur le réseau WAN du service portail.
- PS/WAN-Data – Approvisionnement des adresses IP de réseau WAN-Data de services portail à utiliser pour la création des mappages de conversion CAT vers les dispositif IP de réseau LAN situés dans le secteur d'adresses LAN-Trans.

- Dispositif IP de réseau LAN situé dans le secteur LAN-Trans – Approvisionnement de dispositif IP de réseau LAN avec une adresse IP traduite.
- Dispositif IP de réseau LAN IP situé dans le secteur LAN-Pass – Approvisionnement de dispositif IP de réseau LAN avec une adresse IP qui est transmise par l'intermédiaire du réseau WAN.

L'approvisionnement de la fonctionnalité de câblo-modem est séparée et distincte de l'approvisionnement des services portail et est en dehors du domaine d'application de la présente Recommandation. Le lecteur est prié de consulter les spécifications DOCSIS concernant les descriptions de l'approvisionnement des câblo-modems.

Les éléments fonctionnels dont la liste figure ci-dessus, avec lesquels l'élément de services PS interagit pendant les processus d'approvisionnement, sont identifiés dans la Figure 13-1. L'élément fonctionnel de centre de distribution de clé (KDC, *key distribution centre*) est indiqué en pointillés dans la mesure où il est utilisé dans le mode d'approvisionnement SNMP mais pas en mode d'approvisionnement DHCP. Les autres éléments fonctionnels sont utilisés dans les deux modes d'approvisionnement.

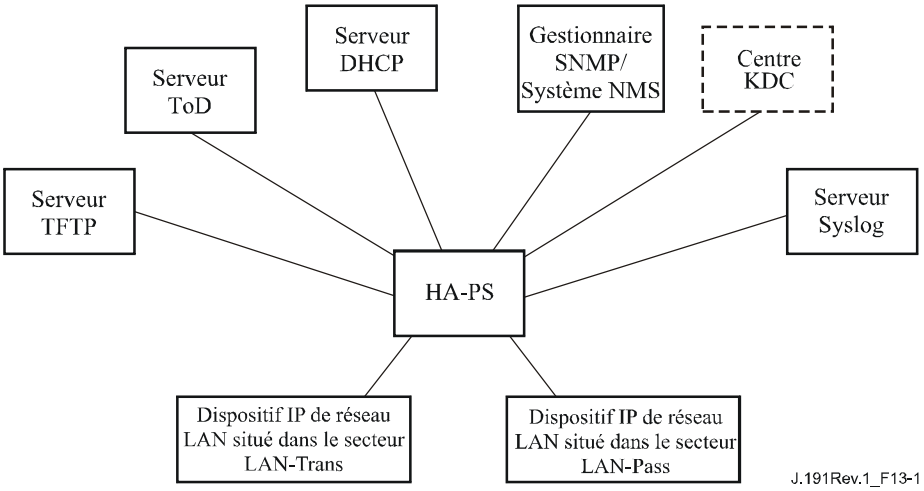


Figure 13-1/J.191 – Eléments fonctionnels d'approvisionnement

Le serveur du protocole trivial de transfert de fichier (TFTP, *trivial file transfer protocol*) donne accès au fichier de configuration PS pour le service portail et suit les règles décrites dans RFC 1350. Le serveur temporel (ToD, *time of day*) fournit au service portail les moyens d'acquérir l'heure actuelle en format UTC, comme décrit dans RFC 868. Le serveur de protocole de configuration de serveur dynamique (DHCP, *dynamic host configuration protocol*) fournit au service portail les adresses IP privées et/ou mondiales selon le document RFC 2131 et fournit également d'autres informations via des options du protocole DHCP conformément au document RFC 2132. Le système de gestion de réseau (NMS)/gestionnaire du protocole simple de gestion de réseau (SNMP) se conforme au document RFC 1157 et éventuellement aux versions plus courantes du protocole SNMP, par exemple [RFC 2576], [RFC 3412], [RFC 3414] et [RFC 3415]. Le centre de distribution de clé (KDC) gère les clés d'autorisation et de chiffrement pour l'établissement de la confiance entre les éléments de réseau et implémente les règles définies dans RFC 1949. Le serveur de journal du système (SYSLOG) traite les messages d'événement produits par le service portail et les dispositifs IP de réseau LAN au domicile. Le service portail implémente les clients de ces serveurs de tête de réseau et utilise ces fonctions de client pendant les processus d'approvisionnement décrits dans le présent paragraphe afin d'accomplir les tâches dont la liste figure au début du présent paragraphe.

13.1 Modes d'approvisionnement

Les § 5.5 et 7.1.1 présentent deux modes d'approvisionnement acceptés par l'élément de services PS: le mode d'approvisionnement DHCP et le mode d'approvisionnement SNMP. Dans le présent paragraphe, chacun des deux modes est présenté plus en détail. La Figure 13-2 illustre un flux d'événements possible dans les deux modes d'approvisionnement. Le point clé de la Figure 13-2 est le commutateur utilisé par le service portail pour déterminer le mode d'approvisionnement dans lequel il doit fonctionner.

Le service portail fonctionne en mode d'approvisionnement DHCP (mode DHCP) si le serveur DHCP dans le réseau câblé fournit une adresse IP valide pour le serveur TFTP dans le champ "siaddr" du message DHCP, s'il fournit un nom de fichier valide pour le fichier de configuration PS dans le champ "file" du message DHCP, et s'il NE fournit PAS la sous-option 51 de l'option 177 du protocole DHCP au client CDC du service portail, pendant la phase DHCPOFFER du processus d'initialisation. Le mode d'approvisionnement DHCP est conçu afin de permettre au service portail de fonctionner sur une infrastructure J.112 avec peu ou pas de changements au réseau DOCSIS.

Le mode d'approvisionnement SNMP du service portail est déclenché lorsque le serveur DHCP du réseau câblé NE fournit PAS de valeurs pour les champs "siaddr" et "file", et lorsque le serveur DHCP du réseau câblé NE fournit PAS la sous-option 51 de l'option 177 du protocole DHCP. Le mode d'approvisionnement SNMP est conçu afin de permettre au service portail de tirer parti des caractéristiques évoluées d'une architecture IPCablecom.

Le service PS passe par défaut au mode CableHome inactif s'il ne reçoit aucun des champs ou des sous-options définis comme étant des déclencheurs des modes d'approvisionnement DHCP et SNMP, ou s'il reçoit une combinaison invalide de ces champs et sous-options.

La Figure 13-2 ci-dessous ne montre pas toutes les conditions d'erreur. Voir au § 7.2.3.3 une description du comportement du service PS en cas de critères incorrects de décision relative au mode d'approvisionnement.

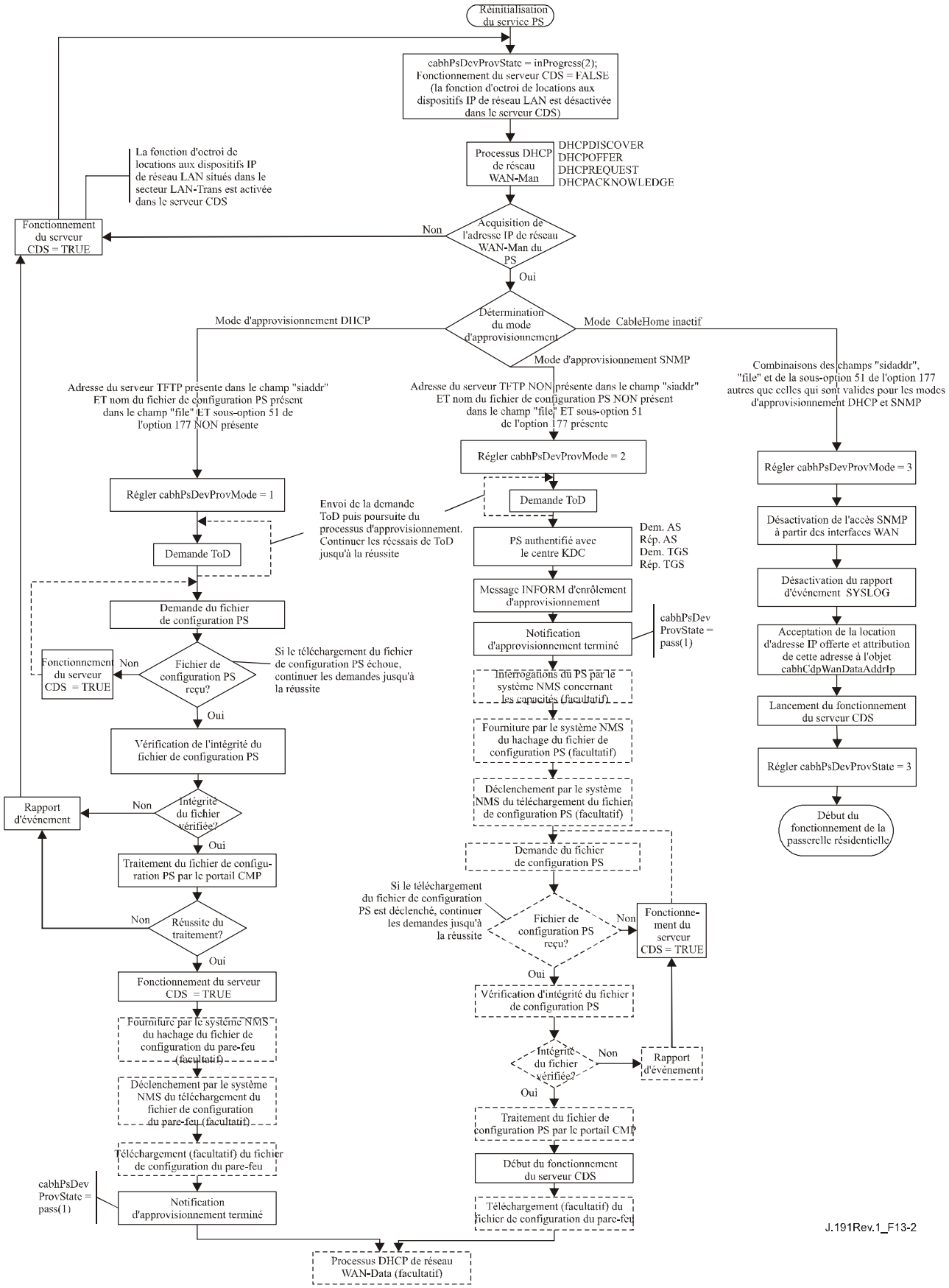


Figure 13-2/J.191 – Modes d'approvisionnement

13.2 Processus d'approvisionnement du service portail pour la gestion en mode d'approvisionnement DHCP

Le service portail demande au système d'approvisionnement de la tête de réseau une adresse IP à utiliser pour l'échange de messages de gestion entre le système NMS et le service portail. Le service portail analyse sémantiquement le message DHCP renvoyé dans le message DHCP OFFER et prend une décision quant au mode d'approvisionnement dans lequel il doit fonctionner (voir § 7.2.3.3). Le paragraphe 7.2.2.2.2 décrit trois modes d'adresse WAN pris en charge pour l'acquisition d'adresses IP par le service portail à partir du serveur DHCP situé dans le réseau câblé.

Si le service portail détermine qu'il doit fonctionner en mode d'approvisionnement DHCP, il utilise les informations du fichier de configuration PS transmises dans le message DHCP comme déclencheur du téléchargement du fichier de configuration PS, comme décrit au § 7.2. Le téléchargement du fichier de configuration PS est nécessaire lorsque le service portail fonctionne en mode d'approvisionnement DHCP mais est facultatif lorsque le service portail fonctionne en mode d'approvisionnement SNMP.

En mode d'approvisionnement DHCP, le service portail (CMP) utilise par défaut le mode NmAccess pour l'échange de messages de gestion avec le système NMS, mais celui-ci a la faculté de configurer le portail CMP en mode de coexistence. Ces modes de messagerie de gestion sont décrits au § 6.3.3.

La Figure 13-3 et le Tableau 13-1 décrivent la séquence des messages nécessaires pour initialiser un service portail fonctionnant en mode d'approvisionnement DHCP. Le processus d'approvisionnement d'un service PS fonctionnant en mode DHCP est le même, que le service PS soit imbriqué avec un câblo-modem ou qu'il soit autonome. L'approvisionnement du service PS imbriqué NE DOIT PAS se produire avant celui du câblo-modem. L'approvisionnement de gestion du service PS autonome DEVRAIT se produire immédiatement après la mise sous tension ou la réinitialisation.

Le processus facultatif de téléchargement d'un fichier de configuration de pare-feu est montré en grisé sur la Figure 13-3.

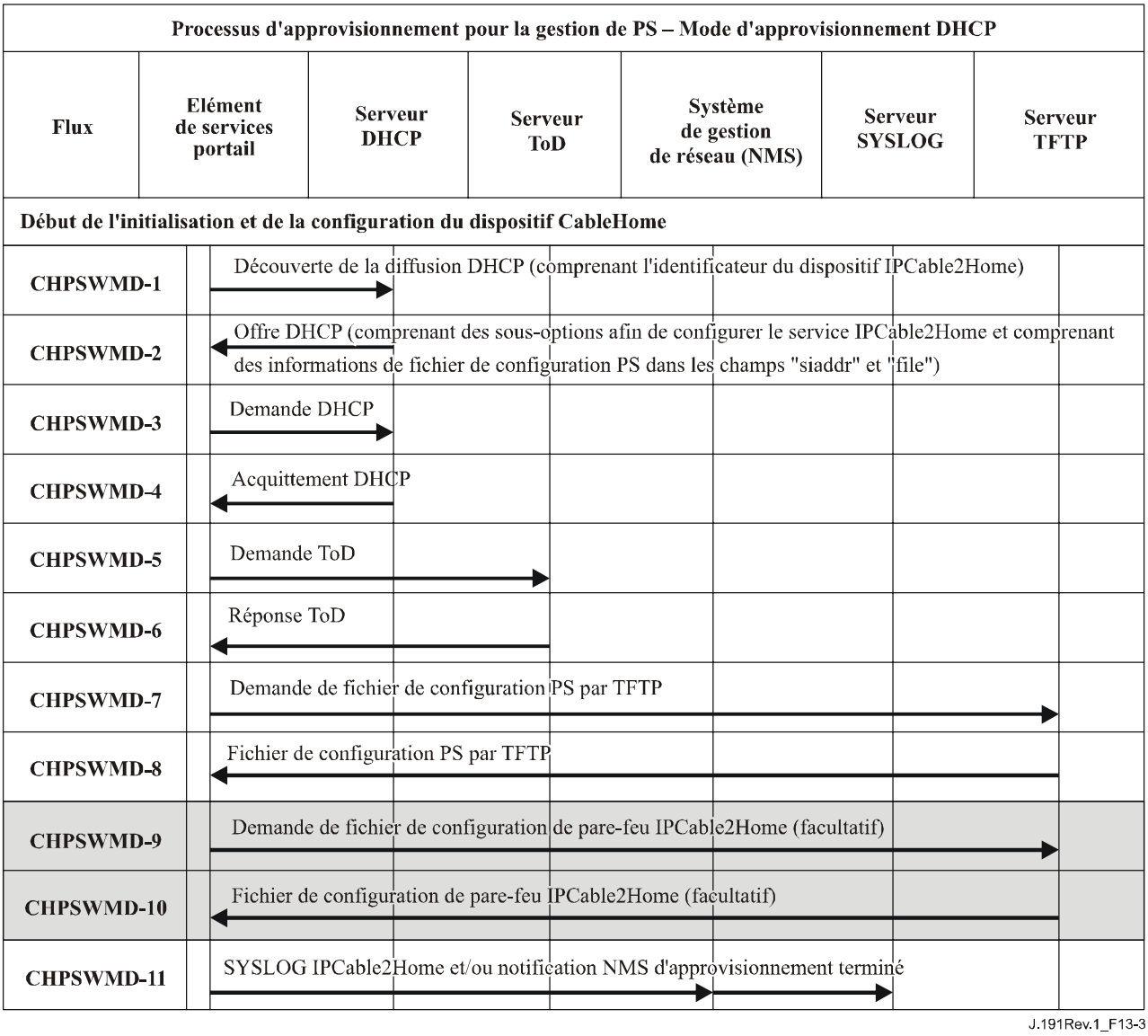


Figure 13-3/J.191 – Processus d'approvisionnement pour la gestion de PS – Mode d'approvisionnement DHCP

Le Tableau 13-1 décrit les messages individuels CHPSWMD-1 à CHPSWMD-11 montrés à la Figure 13-3.

Tableau 13-1/J.191 – Description des flux pour le processus d'approvisionnement WAN-Man du service portail pour le mode d'approvisionnement DHCP

Etape du flux	Approvisionnement WAN-Man des services PS: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
CHPSWMD-1	*DHCP Broadcast Discover (découverte diffusée par DHCP)* Le portail CDP (client CDC) envoie un message DHCP DISCOVER diffusé afin d'acquérir l'adresse IP de réseau WAN-Man comme décrit au § 7.2.3.3. La diffusion du message DHCP DISCOVER par le portail CDP (client CDC) inclut les options obligatoires dont la liste figure au Tableau 7-7. Le service PS règle l'objet cabhPsDevProvState à l'état 'inProgress(2)' lorsque le client CDC diffuse un message DHCP DISCOVER. Le service portail DOIT lancer le temporisateur d'approvisionnement en utilisant la valeur de début qui est accessible via l'objet cabhPsDevProvTimer ET mettre l'objet cabhPsDevProvState à l'état "inProgress" (2) lorsque le client CDC envoie un message DHCP DISCOVER diffusé.	Commencer la séquence d'approvisionnement.	En cas d'échec selon le protocole DHCP, rapporter une erreur et continuer d'essayer de diffuser le message DHCP de découverte jusqu'à la réussite (retourner à l'étape CHPSWMD-1). Si la première tentative pour obtenir une adresse IP de réseau WAN-Man se solde par un échec, le service PS déclenche le fonctionnement du serveur CDS comme précisé au § 7.2.3.3.
CHPSWMD-2	*DHCP OFFER (offre DHCP)* Le message DHCP OFFER produit par le serveur DHCP dans les réseaux câblés est censé ne pas inclure l'option de code 177 contenant les sous-options 3, 6 et 51 ET est censé inclure les informations de fichier de configuration PS dans les champs "siaddr" et "file" du message DHCP. (voir § 7.2.3.3)	CHPSWMD-2 DOIT survenir après achèvement de CHPSWMD-1.	En cas d'échec selon le protocole DHCP, retourner à CHPSWMD-1 et signaler une erreur.
CHPSWMD-3	*DHCP REQUEST (demande DHCP)* Le portail CDP DOIT envoyer au serveur DHCP approprié un message DHCP REQUEST afin de prendre en charge le message DHCP OFFER.	CHPSWMD-3 DOIT survenir après achèvement de CHPSWMD-2.	En cas d'échec selon le protocole DHCP, retourner à CHPSWMD-1 et signaler une erreur.

Tableau 13-1/J.191 – Description des flux pour le processus d'approvisionnement WAN-Man du service portail pour le mode d'approvisionnement DHCP

Etape du flux	Approvisionnement WAN-Man des services PS: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
CHPSWMD-4	*DHCP ACK (acquittement DHCP)* Le serveur DHCP envoie au CDP un message DHCP ACK qui contient l'adresse IPv4 du service PS. Celui-ci modifie l'objet cabhPsDevProvMode sur la base des informations reçues dans le message DHCP ACK (voir § 7.2.3.3). Le service PS mémorise l'adresse du serveur temporel dans l'objet cabhPsDevTimeServerAddr.	CHPSWMD-4 DOIT survenir après achèvement de CHPSWMD-3.	En cas d'échec selon le protocole DHCP, retourner à CHPSWMD-1 et signaler une erreur. Si les informations attendues du fichier de configuration ne sont pas reçues dans le message DHCP ACK après 5 tentatives, le service PS fonctionne en "mode CableHome inactif" comme décrit dans les § 5.5 et 7.2.3.3.
CHPSWMD-5	*Demande d'heure (ToD) selon RFC 868* Le service PS envoie une demande d'heure au serveur temporel identifié dans le message DHCP OFFER.	CHPSWMD-5 DOIT survenir après achèvement de l'étape CHPSWMD-4.	Passer à l'étape CHPSWMD-6.
CHPSWMD-6	*Réponse d'heure ToD* Le serveur temporel est censé répondre avec l'heure actuelle en format UTC.	CHPSWMD-6 DOIT survenir après achèvement de CHPSWMD-5.	Passer à l'étape CHPSWMD-7, signaler une erreur, et retourner à CHPSWMD-5 (continuer d'essayer l'heure ToD jusqu'à réussite).
CHPSWMD-7	*Demande TFTP* Le service PS fonctionnant en mode d'approvisionnement DHCP envoie au serveur TFTP une demande TFTP Get (requête) afin de demander le fichier de données de configuration spécifié comme décrit au § 7.3.3.	CHPSWMD-7 DOIT survenir après achèvement de CHPSWMD-5. CHPSWMD-7 PEUT survenir avant l'achèvement de CHPSWMD-6.	Passer à l'étape CHPSWMD-8.

Tableau 13-1/J.191 – Description des flux pour le processus d'approvisionnement WAN-Man du service portail pour le mode d'approvisionnement DHCP

Etape du flux	Approvisionnement WAN-Man des services PS: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
CHPSWMD-8	*Le serveur TFTP envoie le fichier de configuration PS* Après réception du fichier de configuration, le hachage du fichier de configuration PS est vérifié (voir le § 7.3.3.3) puis est traité. Voir au § 7.3.3 le contenu du fichier de configuration PS. Facultativement, l'adresse IP du serveur TFTP de fichier de configuration de pare-feu, le nom du fichier de configuration du pare-feu et le hachage du fichier de configuration du pare-feu sont inclus dans le fichier de configuration PS s'il y a un fichier de configuration de pare-feu à charger, et c'est la méthode choisie pour le spécifier.	CHPSWMD-8 DOIT survenir après achèvement de CHPSWMD-7.	Si le téléchargement TFTP échoue, signaler une erreur et retourner à CHPSWMD-7 (continuer d'essayer de télécharger le fichier de configuration PS). Si le traitement du fichier de configuration PS produit une erreur, passer à l'étape CHPSWMD-9 et rapporter l'erreur comme événement. Si le temporisateur d'approvisionnement arrive à expiration avant que le fichier de configuration PS soit bien téléchargé, le PS DOIT rapporter une erreur et retourner à l'étape CHPSWMD-1.
CHPSWMD-9	*Demande TFTP – Fichier de configuration de pare-feu (facultatif)* Si le service PS reçoit des informations de fichier de configuration de pare-feu (serveur TFTP de pare-feu et nom de fichier de configuration de pare-feu) dans le fichier de configuration PS, le service PS envoie au serveur TFTP de configuration de pare-feu une requête TFTP GET afin de demander un fichier de configuration de pare-feu (voir le § 11.3.5.1). Si le service PS ne reçoit pas d'information de fichier de configuration de pare-feu dans le fichier de configuration PS, le processus d'approvisionnement du service portail (mode d'approvisionnement DHCP) DOIT sauter les étapes CHPSWMD-9 et CHPSWMD-10 et passer à l'étape CHPSWMD-11.	Si l'étape CHPSWMD-9 se produit, elle DOIT survenir après achèvement de CHPSWMD-8.	Si le transfert TFTP échoue, continuer le fonctionnement du service portail mais signaler une erreur et continuer d'essayer CHPSWMD-9.

Tableau 13-1/J.191 – Description des flux pour le processus d'approvisionnement WAN-Man du service portail pour le mode d'approvisionnement DHCP

Etape du flux	Approvisionnement WAN-Man des services PS: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
CHPSWMD-10	*Le serveur TFTP envoie un fichier de configuration de pare-feu (facultatif)* Si l'étape CHPSWMD-9 se produit, le serveur TFTP envoie au service PS une réponse TFTP contenant le fichier demandé. Après réception du fichier de configuration de pare-feu, le hachage du fichier de configuration PS est calculé et comparé à la valeur reçue dans le fichier de configuration PS. Le fichier est ensuite traité. Voir le § 11.3.5.	CHPSWMD-10 DOIT survenir après achèvement de CHPSWMD-9.	Si le transfert TFTP échoue, continuer le fonctionnement du service portail mais signaler une erreur et continuer d'essayer CHPSWMD-9. Si le traitement du fichier de configuration de pare-feu produit une erreur, continuer et rapporter l'erreur comme événement.
CHPSWMD-11	*Approvisionnement terminé* Sur demande du système d'approvisionnement, le service PS est tenu d'informer le système d'approvisionnement de l'état de l'approvisionnement des services PS. Le système d'approvisionnement peut demander au service PS d'envoyer un message SYSLOG ou un transfert SNMP, ou les deux. Si le service PS mène à bien toutes les étapes requises de CHPSWMD-1 à CHPSWMD-10 ET qu'il reçoive une adresse de serveur SYSLOG dans le message DHCP OFFER, ce service PS DOIT envoyer un message d'approvisionnement terminé au serveur SYSLOG avec l'état d'approvisionnement mis à PASS (*réussi*).	CHPSWMD-11 DOIT survenir après achèvement de CHPSWMD-10.	Si le transfert SNMP échoue, le serveur d'approvisionnement ne peut pas savoir que le processus d'approvisionnement est terminé à moins qu'il n'interroge l'objet cabhPsProvState.

Tableau 13-1/J.191 – Description des flux pour le processus d'approvisionnement WAN-Man du service portail pour le mode d'approvisionnement DHCP

Etape du flux	Approvisionnement WAN-Man des services PS: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
	Si le service PS mène à bien toutes les étapes d'approvisionnement requises de CHPSWMD-1 à CHPSWMD-10 ET qu'il reçoive des paramètres valides pour l'objet docsDevNmAccessGroup identifiant le récepteur de transferts (objet docsDevNmAccessIP) et configurant le transfert d'achèvement d'approvisionnement (objet cabhPsDevInitTrap) en "lecture seule avec les transferts" (commande docsDevNmAccess mise à "4", voir le document RFC 2669), le service PS DOIT envoyer au récepteur de transferts un message TRAP d'approvisionnement terminé (objet cabhPsDevInitTrap) avec les paramètres appropriés. Si le temporisateur d'approvisionnement PS arrive à expiration avant l'achèvement de toutes les étapes requises de CHPSWMD-1 à CHPSWMD-10 ET que le service PS reçoive une adresse de serveur SYSLOG dans le message DHCP OFFER, le service PS DOIT envoyer un message approvisionnement terminé au serveur SYSLOG avec l'état d'approvisionnement mis à FAIL. Si le temporisateur d'approvisionnement PS arrive à expiration avant l'achèvement de toutes les étapes requises de CHPSWMD-1 à CHPSWMD-10 ET si le service PS a reçu des paramètres valides pour le récepteur de notification, le service PS DOIT envoyer au récepteur de notifications une notification d'échec d'approvisionnement (objet cabhPsDevInitTrap).		

Tableau 13-1/J.191 – Description des flux pour le processus d'approvisionnement WAN-Man du service portail pour le mode d'approvisionnement DHCP

Etape du flux	Approvisionnement WAN-Man des services PS: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
	Le service PS DOIT mettre à jour la valeur de l'objet cabhPsDevProvState avec l'état 'pass' (1) lorsque les étapes de flux d'approvisionnement CHPSWMD-1 à CHPSWMD-11 ont été menées à bien. Le service PS DOIT mettre à jour la valeur de l'objet cabhPsDevProvState avec l'état 'fail' (3) ET signaler d'un événement indiquant l'échec du processus d'approvisionnement si le temporisateur d'approvisionnement PS arrive à expiration avant que la valeur de l'objet cabhPsDevProvState ne soit mise à jour avec l'état "pass".		

13.3 Processus d'approvisionnement du service portail pour la gestion en mode d'approvisionnement SNMP

Le service portail demande au serveur DHCP de tête de réseau une adresse de couche Réseau WAN-Man destinée aux échanges de messages de gestion entre les fonctions de gestion de services portail et le système NMS du réseau câblé. Si le service portail détermine sur la base de la procédure décrite au § 7.3.3.3 qu'il doit fonctionner en mode d'approvisionnement SNMP, le service portail sécurisera ses messages de gestion en utilisant SNMPv3 conformément à la procédure d'authentification décrite au § 11.3.3.

Le système NMS du réseau câblé peut facultativement donner pour instruction au service portail (CMP) fonctionnant en mode d'approvisionnement SNMP de télécharger un fichier de configuration PS à partir du serveur TFTP. La notification d'achèvement du processus d'approvisionnement est fournie au moyen du processus de rapport d'événement décrit au § 6.5.

La Figure 13-4 illustre les flux de messages qui servent à mettre en œuvre l'approvisionnement du service portail lorsqu'il fonctionne en mode d'approvisionnement SNMP. Le processus d'approvisionnement à l'interface PS/WAN-Man est le même pour le service PS imbriqué et pour le service PS autonome. L'approvisionnement du service PS autonome DEVRAIT intervenir immédiatement après la mise sous tension/réinitialisation.

Le processus d'approvisionnement pour l'interface entre un réseau WAN-Man et un service PS fonctionnant en mode d'approvisionnement SNMP DOIT intervenir via la séquence décrite à la Figure 13-4 et détaillée au Tableau 13-2. Les étapes facultatives sont indiquées en grisé dans la Figure 13-4 et peuvent être franchies immédiatement après l'étape CHPSWMS-13, ultérieurement, ou pas du tout.

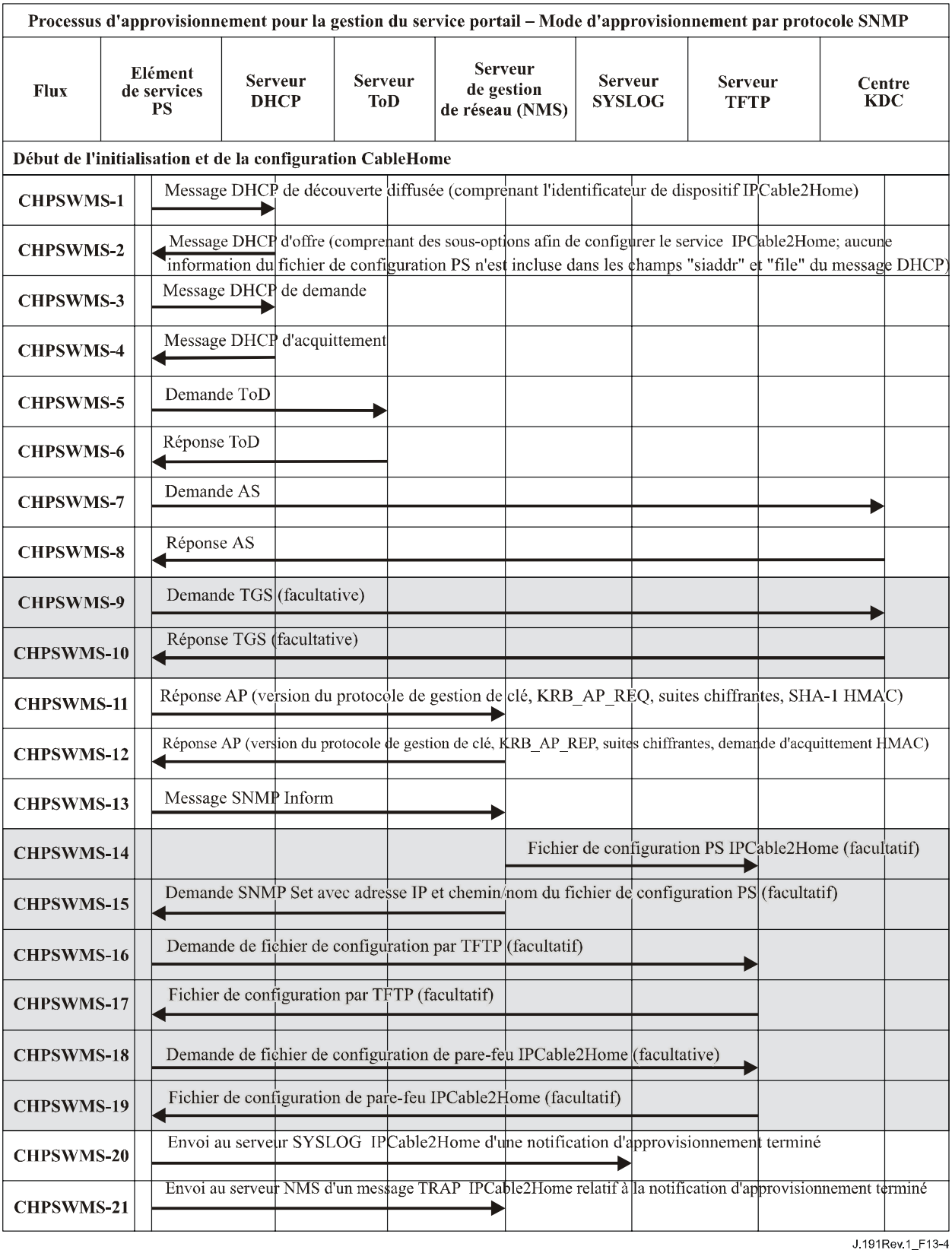


Figure 13-4/J.191 – Processus d'approvisionnement pour la gestion du service portail – Mode d'approvisionnement par protocole SNMP

Le Tableau 13-2 décrit les étapes individuelles du processus d'approvisionnement montré à la Figure 13-4.

Tableau 13-2/J.191 – Description des flux pour le processus d'approvisionnement du service portail par secteur WAN-Man pour la gestion en mode d'approvisionnement SNMP

Etape de flux	Approvisionnement WAN-Man de PS: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
CHPSWMS-1	*Message DHCP de découverte diffusé* Le portail CDP (client CDC) diffuse un message DHCP DISCOVER afin d'acquérir l'adresse IP du réseau WAN-Man comme décrit au § 7.2.3. La diffusion du message DHCP DISCOVER par le portail CDP (client CDC) inclut les options DHCP obligatoires de client CDC dont la liste figure au Tableau 7-7. Le service PS commence à surveiller la durée écoulée ET règle l'objet cabhPsDevProvState à l'état 'inProgress' (2) lorsque le client CDC diffuse son message DHCP DISCOVER initial.	Début de la séquence d'approvision-nement	S'il y a échec selon le protocole DHCP, signaler l'erreur et continuer à essayer de diffuser le message DHCP DISCOVER jusqu'à la réussite (retourner à l'étape CHPSWMS-1). En cas d'échec de la première tentative d'acquérir une location d'adresse à partir du serveur DHCP de la tête de réseau, initialiser le fonctionnement du serveur CDS comme spécifié au § 7.2.3.3.
CHPSWMS-2	*DHCP OFFER* Le message DHCP OFFER produit par le serveur DHCP dans le réseau câblé est censé inclure le code d'option 177 avec les sous-options 3, 6 et 51 ET aucune information de fichier de configuration PS dans les champs "siaddr" et "file" du message DHCP.	CHPSWMS-2 DOIT survenir après achèvement de CHPSWMS-1.	S'il y a échec selon le protocole DHCP, retourner à CHPSWMS-1 et signaler l'erreur.
CHPSWMS-3	*DHCP REQUEST* Le client CDC envoie au serveur DHCP approprié un message DHCP REQUEST afin de prendre en charge l'offre DHCP OFFER.	CHPSWMS-3 DOIT survenir après achèvement de CHPSWMS-2.	S'il y a échec selon le protocole DHCP, retourner à CHPSWMS-1.
CHPSWMS-4	*DHCP ACK* Le serveur DHCP envoie au client CDC un message d'acquittement DHCP ACK qui contient l'adresse IPv4 de l'interface PS/WAN-Man et est censé inclure l'option CableHome 177 avec les sous-options 3, 6 et 51 ET aucune information de fichier de configuration PS dans les champs 'siaddr' et 'file' du message DHCP. Le service PS modifie l'objet cabhPsDevProvMode sur la base des informations reçues dans le message DHCP ACK (voir § 7.2.3.3).	CHPSWMS-4 DOIT survenir après achèvement de CHPSWMS-3.	S'il y a échec selon le protocole DHCP, retourner à l'étape CHPSWMS-1 et signaler l'erreur.

Tableau 13-2/J.191 – Description des flux pour le processus d'approvisionnement du service portail par secteur WAN-Man pour la gestion en mode d'approvisionnement SNMP

Etape de flux	Approvisionnement WAN-Man de PS: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
	Le service PS mémorise l'adresse du serveur temporel dans l'objet cabhPsDevTimeServerAddr.		
CHPSWMS-5	*Demande d'heure (ToD) selon RFC 868* Le service PS envoie une demande d'heure au serveur ToD identifié dans le message DHCP ACK.	CHPSWMS-5 DOIT survenir après achèvement de CHPSWMS-4.	Passer à l'étape CHPSWMS-6.
CHPSWMS-6	*Réponse d'heure (ToD)* Le serveur temporel est censé répondre avec l'heure actuelle en format UTC.	CHPSWMS-6 DOIT survenir après achèvement de CHPSWMS-5.	Passer à l'étape CHPSWMS-7, signaler l'erreur, et retourner à CHPSWMS-5 (continuer à essayer l'heure jusqu'à réussite).
CHPSWMS-7	*Demande de serveur d'application AS (Note)* Le service PS envoie le message de demande de serveur d'application au centre KDC de l'opérateur IPCable2Home afin de demander un ticket Kerberos.	CHPSWMS-7 DOIT survenir après achèvement de CHPSWMS-6.	Retourner à CHPSWMS-1. Le service PS lance le fonctionnement du serveur CDS.
CHPSWMS-8	*Réponse de serveur d'application AS* Le message de réponse de serveur d'application est reçu du centre KDC de l'opérateur IPCable2Home qui contient le ticket Kerberos.	CHPSWMS-8 DOIT survenir après achèvement de CHPSWMS-7.	Retourner à CHPSWMS-1. Le service PS lance le fonctionnement du serveur CDS.
CHPSWMS-9	*Demande (facultative) de serveur TGS* Si le service PS a obtenu un ticket d'attribution de ticket (TGT, *ticket granting ticket*) dans l'étape CHPSWMS-8, le service PS envoie le message de demande de serveur TGS au serveur de centre KDC de l'opérateur dont l'adresse a été transmise au service PS (client CDC) dans la sous-option 51 de l'option DHCP 177.	CHPSWMS-9 DOIT survenir après achèvement de CHPSWMS-8.	Retourner à CHPSWMS-1. Le service PS lance le fonctionnement du serveur CDS.
CHPSWMS-10	*Réponse (facultative) de serveur TGS* Le message de réponse de serveur TGS contenant le ticket est reçu du centre KDC de l'opérateur.	CHPSWMS-10 DOIT survenir après achèvement de CHPSWMS-9.	Retourner à CHPSWMS-1. Le service PS lance le fonctionnement du serveur CDS.

Tableau 13-2/J.191 – Description des flux pour le processus d'approvisionnement du service portail par secteur WAN-Man pour la gestion en mode d'approvisionnement SNMP

Etape de flux	Approvisionnement WAN-Man de PS: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
CHPSWMS-11	*Demande de point d'accès AP* Le message de demande de point d'accès est envoyé par le service PS au serveur NMS (gestionnaire SNMP) afin de demander les informations sur les clés pour la version SNMPv3 comme décrit au § 11.3.3.2.	CHPSWMS-11 DOIT survenir après achèvement de CHPSWMS-10.	Retourner à CHPSWMS-1. Le service PS lance le fonctionnement du serveur CDS.
CHPSWMS-12	*Réponse de point d'accès AP* Le message de réponse de point d'accès est reçu du serveur NMS contenant les informations sur les clés pour la version SNMPv3. NOTE – Le service PS DOIT établir les clés SNMPv3 et remplir les tables SNMPv3 associées avant d'envoyer un message INFORM conforme à SNMPv3. Les clés et les tables sont établies au moyen des informations contenues dans la réponse AP (voir de plus amples détails au § 11.3).	CHPSWMS-12 DOIT survenir après achèvement de CHPSWMS-11.	Retourner à CHPSWMS-1. Le service PS lance le fonctionnement du serveur CDS.
CHPSWMS-13	*SNMP INFORM* Après avoir établi les clés SNMPv3, le service PS fonctionnant en mode d'approvisionnement SNMP DOIT envoyer un message INFORM selon SNMPv3 (objet cabhPsDevProvEnrollTrap) afin de demander l'enrôlement dans l'entité SNMP dont l'adresse IP a été fournie dans la sous-option 3 de l'option 177, contenue dans le message DHCP ACK.	CHPSWMS-13 DOIT survenir après achèvement de CHPSWMS-12.	Retourner à CHPSWMS-1.

Tableau 13-2/J.191 – Description des flux pour le processus d'approvisionnement du service portail par secteur WAN-Man pour la gestion en mode d'approvisionnement SNMP

Etape de flux	Approvisionnement WAN-Man de PS: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
CHPSWMS-14	*Création (facultative) du fichier de configuration* Le système d'approvisionnement utilise les informations issues des précédentes étapes d'approvisionnement du service PS afin de créer un fichier de configuration PS. Le système d'approvisionnement effectue un hachage sur le contenu de ce fichier de configuration. La valeur de ce hachage est envoyée au service PS lors de l'étape suivante.	Si l'étape CHPSWMS-14 se produit, elle DOIT survenir après achèvement de CHPSWMS-13.	N/A
CHPSWMS-15	*Commande (facultative) SET du protocole SNMP* Le système d'approvisionnement peut commander au système NMS d'envoyer au service PS un message SNMP SET contenant l'adresse IP du serveur TFTP, le nom du fichier de configuration PS et la valeur de hachage du fichier de configuration comme décrit au § 7.3.3.2 (mode d'approvisionnement SNMP). En variante, l'adresse IP du serveur TFTP du fichier de configuration du pare-feu, le nom du fichier de configuration du pare-feu et la valeur de hachage du fichier de configuration du pare-feu peuvent être inclus dans la commande SET du protocole SNMP s'il existe un fichier de configuration de pare-feu à charger. Cette méthode est choisie afin de spécifier cela.	Si l'étape CHPSWMS-15 se produit, elle DOIT survenir après achèvement de CHPSWMS-14.	Retourner à CHPSWMS-1 si la commande SET a été reçue mais qu'une erreur de traitement se soit produite.
CHPSWMS-16	*Demande (facultative) de transfert TFTP* Si le système NMS déclenche le téléchargement par le service PS d'un fichier de configuration PS comme décrit au § 7.3.3.2, le service PS envoie au serveur TFTP une demande TFTP GET afin de demander le fichier de configuration PS spécifié.	Si l'étape CHPSWMS-16 se produit, elle DOIT survenir après achèvement de l'étape CHPSWMS-15.	Passer à l'étape CHPSWMS-17.

Tableau 13-2/J.191 – Description des flux pour le processus d'approvisionnement du service portail par secteur WAN-Man pour la gestion en mode d'approvisionnement SNMP

Etape de flux	Approvisionnement WAN-Man de PS: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
CHPSWMS-17	*Envoi (facultatif) du fichier de configuration par le serveur TFTP* Après avoir reçu le fichier de configuration PS, le service PS calcule le hachage du fichier de configuration PS et le compare à la valeur reçue dans l'étape CHPSWMS-15. Le service PS traite alors le fichier de configuration PS. Voir au § 7.3.3 le contenu du fichier de configuration PS. Facultativement, l'adresse IP du serveur TFTP du fichier de configuration du pare-feu, le nom du fichier de configuration du pare-feu et le hachage du fichier de configuration du pare-feu sont inclus dans le fichier de configuration PS s'il y a un fichier de configuration de pare-feu à charger, et cette méthode est choisie pour spécifier cela.	Si l'étape CHPSWMS-17 se produit, elle DOIT survenir après achèvement de CHPSWMS-16.	Si le téléchargement TFTP échoue, signaler une erreur, passer à l'étape CHPSWMS-18 et continuer d'essayer CHPSWMS-16 (continuer d'essayer le téléchargement du fichier de configuration PS). Si le traitement du fichier de configuration produit une erreur, continuer et signaler l'erreur comme un événement.
CHPSWMS-18	*Demande (facultative) TFTP – Fichier de configuration de pare-feu* Le service PS envoie au serveur TFTP de configuration de pare-feu une demande TFTP Get afin de demander le fichier de données de configuration de pare-feu spécifié.	Si l'étape CHPSWMS-18 se produit, elle DOIT survenir après achèvement de l'étape CHPSWMS-17.	Passer à l'étape CHPSWMS-19.
CHPSWMS-19	*Envoi (facultatif) du fichier de configuration de pare-feu par le serveur TFTP* Le serveur TFTP envoie au service PS une réponse TFTP contenant le fichier demandé. Après réception du fichier de configuration de pare-feu par le service PS, celui-ci calcule le hachage du fichier de configuration du pare-feu et le compare à la valeur reçue à l'étape CHPSWMS-15 ou 17. Le fichier est ensuite traité. Voir de plus amples détails au § 11.3.	Si l'étape CHPSWMS-19 se produit, elle DOIT survenir après achèvement de l'étape CHPSWMS-18.	Si le téléchargement TFTP échoue, continuer le fonctionnement du service portail mais signaler une erreur et continuer d'essayer CHPSWMS-18. Si le traitement du fichier de configuration de pare-feu produit une erreur, continuer et signaler l'erreur comme un événement.

Tableau 13-2/J.191 – Description des flux pour le processus d'approvisionnement du service portail par secteur WAN-Man pour la gestion en mode d'approvisionnement SNMP

Etape de flux	Approvisionnement WAN-Man de PS: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
CHPSWMS-20	*Notification SYSLOG* Si le service PS a reçu une adresse de serveur SYSLOG dans le message DHCP ACK, le service PS DOIT envoyer au serveur SYSLOG une notification "d'approvisionnement terminé". Le format général de cette notification a été défini au § 6.5.1.	CHPSWMS-20 DOIT survenir après achèvement de CHPSWMS-19.	N/A
CHPSWMS-21	*Message TRAP du protocole SNMP* Le service PS DOIT envoyer au système NMS un message TRAP du protocole SNMP (objet cabhPsDevInitTrap) contenant une notification "d'approvisionnement terminé". Un état FAIL (échec) se produit si le traitement du fichier de configuration échoue. Sinon, l'état d'approvisionnement est PASS (succès). Le service PS DOIT mettre à jour la valeur de l'objet cabhPsDevProvState à l'état 'pass' (1) lorsque les étapes de flux CHPSWMS-1 à 13 s'achèvent correctement. Le service PS DOIT mettre à jour la valeur de l'objet cabhPsDevProvState à l'état 'fail' (3) ET signaler un événement indiquant un échec du processus d'approvisionnement si le temporisateur d'approvisionnement du service PS arrive à expiration avant que la valeur de l'objet cabhPsDevProvState soit mis à jour par la valeur d'état 'pass'.	CHPSWMS-21 DOIT survenir après achèvement de CHPSWMS-20.	N/A
NOTE – Les étapes CHPSWMS-5 à CHPSWMS-8 sont facultatives dans certains cas. Voir les détails au § 11.			

13.3.1 Téléchargement de fichier de configuration PS/WAN-Man

Le service portail fonctionnant en mode d'approvisionnement SNMP PEUT contenir suffisamment d'informations par défaut d'usine afin de permettre le fonctionnement du côté LAN ou du côté WAN ou des deux côtés sans téléchargement de fichier de configuration PS. Si le service portail fonctionne en mode d'approvisionnement SNMP, le fichier de configuration PS PEUT être téléchargé pour l'approvisionnement initial afin de remplacer les valeurs par défaut d'usine ou afin de fournir des informations complémentaires.

Le fichier de configuration de pare-feu contient les informations permettant fournir la fonction de pare-feu. L'indication de téléchargement du fichier de configuration PS viendra soit dans le fichier de configuration PS soit via une commande SNMP Set pendant l'initialisation.

13.3.2 Temporisateur d'approvisionnement de services portail

Un temporisateur d'approvisionnement est fourni afin de garantir que le service portail continuera de poursuivre le processus d'approvisionnement même si une opération ne se termine pas. L'objet de temporisateur, cabhPsDevProvTimer, a une durée initiale par défaut de 5 minutes.

13.3.3 Messages INFORM d'enrôlement d'approvisionnement/approvisionnement terminé

Pour le service portail fonctionnant seulement en mode d'approvisionnement SNMP, le message INFORM d'enrôlement d'approvisionnement (objet cabhPsDevProvEnrollTrap) permet au serveur d'approvisionnement de déterminer si le service portail est prêt pour le fichier de configuration PS.

Aussi bien en mode d'approvisionnement DHCP qu'en mode d'approvisionnement SNMP, le transfert d'approvisionnement terminé (objet cabhPsDevInitTrap) indique si la séquence d'approvisionnement a été ou non menée à bien.

13.3.4 Approvisionnement d'enregistrement SYSLOG

L'adresse IP du serveur syslog DOIT être approvisionnée à travers le processus DHCP. L'événement d'enregistrement syslog ne sera pas envoyé si l'adresse IP du serveur syslog n'est pas configurée.

13.3.5 Etat d'approvisionnement et rapport d'erreur

Comme indiqué dans les Tableaux 13-1 et 13-2, un échec au cours des étapes du processus d'approvisionnement provoque généralement le redémarrage du processus à la première étape, CHPSWMD-1 ou CHPSWMS-1.

13.4 Processus d'approvisionnement PS/WAN-Data

Le service portail demande zéro, une ou plusieurs adresses de réseau WAN-Data au serveur DHCP se trouvant dans le réseau câblé. Ces adresses sont destinées à être utilisées pour l'échange des données entre les éléments connectés au réseau Internet et les dispositifs IP de réseau LAN.

Il n'y a pas de différence entre les modes d'approvisionnement DHCP et SNMP en termes de fonctionnement PS/WAN-Data.

Les diagrammes ci-après illustrent les flux de messages qui doivent être utilisés pour mettre en œuvre l'approvisionnement des adresses PS/WAN-Data. Le processus d'approvisionnement pour les adresses PS/WAN-Data est le même pour le service PS imbriqué avec un câblo-modem que pour le service PS autonome.

Si le processus d'approvisionnement pour la ou les adresses PS/WAN-Data se produit, il DOIT suivre la séquence décrite à la Figure 13-5, qui est détaillée dans le Tableau 13-3.

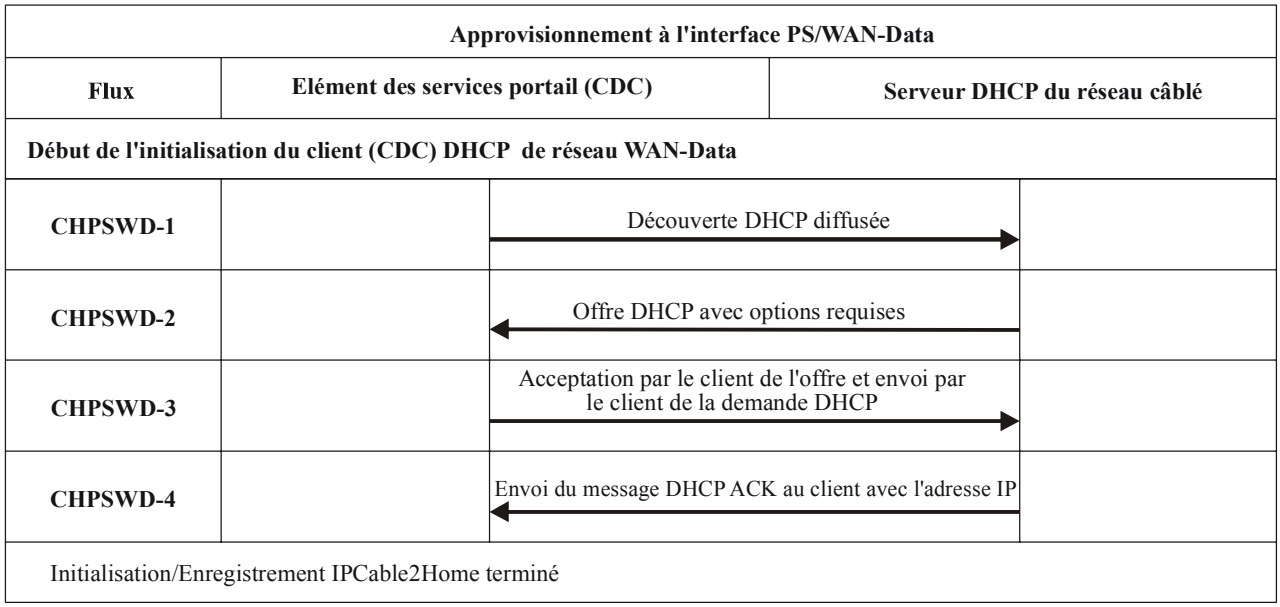


Figure 13-5/J.191 – Processus d'approvisionnement PS/WAN-Data

Tableau 13-3/J.191 – Description des flux pour le processus d'approvisionnement du service portail par secteur WAN-Data

Etape de flux	Approvisionnement d'adresse PS/WAN-Data	Séquence normale	Séquence d'échec
CHPSWD-1	*Message DHCP DISCOVER en diffusion* Le service PS diffuse un message DHCP DISCOVER incluant les options obligatoires énumérées au Tableau 7-7.	Passer à l'étape CHPSWD-2.	En cas d'échec selon le protocole DHCP, répéter CHPSWD-1.
CHPSWD-2	*Message DHCP OFFER* Le serveur DHCP situé à la tête de réseau reçoit le paquet DHCP DISCOVER, attribue une adresse IP extraite de la réserve WAN-Data, construit un paquet DHCP OFFER, et transmet l'offre DHCP OFFER à l'agent de relais DHCP situé dans le système CMTS.	Passer à l'étape CHPSWD-3.	En cas d'échec, le client arrivera en fin de temporisation selon le protocole DHCP et l'étape CHPSWD-1 sera répétée.
CHPSWD-3	*Message DHCP REQUEST* Le portail CDP envoie au serveur DHCP choisi un message DHCP REQUEST afin d'accepter l'offre DHCP OFFER.	CHPSWD-3 DOIT survenir après achèvement de CHPSWD-2.	En cas d'échec selon le protocole DHCP, retourner à CHPSWD-1.
CHPSWD-4	*Message DHCP ACK* Le serveur DHCP envoie au portail CDP un message d'acquittement DHCP ACK qui contient l'adresse IPv4 pour l'interface PS/WAN-Data.	CHPSWD-4 DOIT survenir après achèvement de CHPSWD-3. L'approvisionnement se termine avec l'achèvement de CHPSWD-4.	En cas d'échec selon le protocole DHCP, retourner à CHPSWD-1.

13.5 Processus d'approvisionnement: client DHCP dans le secteur LAN-Trans

Les dispositifs IP de réseau LAN demandent des adresses IP via les processus DHCP. L'élément de services PS traite ces messages conformément aux paramètres d'approvisionnement attribués par le système NMS du réseau câblé (voir § 7.2.3.2).

Le présent paragraphe décrit le processus d'approvisionnement dans le cas où le système NMS a approvisionné le service portail de façon à fonctionner en mode de traitement primaire de paquet par conversion C-NAT ou C-NAPT (voir § 8). Il n'y a pas de différence entre les modes d'approvisionnement DHCP et SNMP en termes de processus d'approvisionnement de dispositif IP de secteur LAN-Trans.

Les flux de messages du processus d'approvisionnement pour un dispositif IP de réseau LAN situé dans le secteur d'adresses LAN-Trans sont décrits à la Figure 13-6. Des détails supplémentaires sur le processus sont fournis au Tableau 13-4.

Le processus d'approvisionnement pour le dispositif IP de réseau LAN situé dans le secteur LAN-Trans DOIT survenir via la séquence décrite à la Figure 13-6 et détaillée au Tableau 13-4.

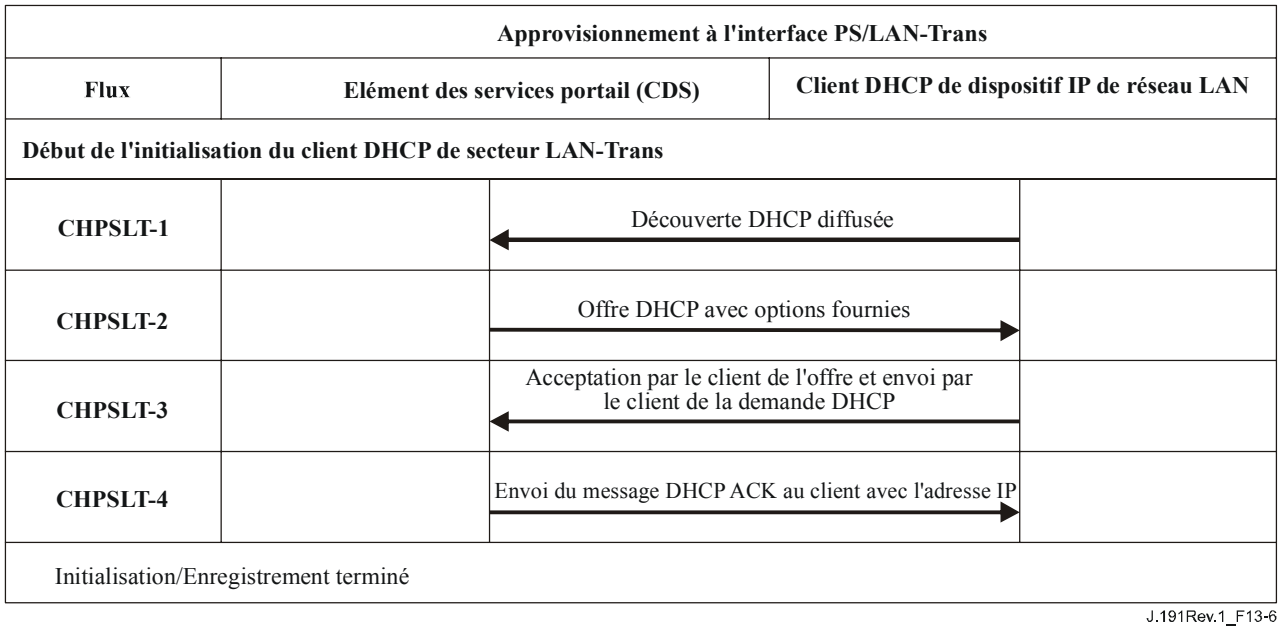


Figure 13-6/J.191 – Processus d'approvisionnement pour dispositif IP de réseau LAN situé dans le secteur LAN-Trans

Tableau 13-4/J.191 – Description des flux pour le processus d'approvisionnement du service portail par secteur LAN-Trans

Etape de flux	Approvisionnement du client d'adresse LAN-Trans	Séquence normale	Séquence d'échec
CHPSLT-1	*Message DHCP DISCOVER en diffusion* Le client (Note 1) diffuse un message DHCP DISCOVER sur son réseau LAN (Note 2) local.	Passer à l'étape CHPSLT-2.	En cas d'échec selon le protocole DHCP, répéter CHPSLT-1.
CHPSLT-2	*Message DHCP OFFER* Le service PS reçoit le message DHCP DISCOVER à son interface avec le réseau LAN et examine le champ *chaddr*. – s'il y a une adresse LAN-Trans disponible et – s'il n'y a pas de considérations administratives justifiant le rejet de l'adresse LAN-Trans pour le client, le service PS DOIT alors envoyer un message DHCP OFFER au client pour lui offrir l'adresse LAN-Trans soit en unidiffusion soit en diffusion sur liaison spécifique (conformément au bit BROADCAST du champ de fanions du message DHCP DISCOVER).	Passer à l'étape CHPSLT-3.	En cas d'échec, le client dépassera la temporisation selon le protocole DHCP et CHPSLT-1 sera répétée.
CHPSLT-3	*DHCP REQUEST* Le client DHCP du dispositif IP de réseau LAN reçoit le message DHCP OFFER. Lorsqu'un client DHCP de dispositif IP de réseau LAN souhaite accepter une offre DHCP OFFER, il est censé formater et envoyer un paquet de demande DHCP REQUEST en utilisant la diffusion sur liaison spécifique (Note 3).	Passer à l'étape CHPSLT-4.	En cas d'échec, le client dépassera la temporisation selon le protocole DHCP et CHPSLT-1 sera répétée.
CHPSLT-4	*DHCP ACK* Le service PS reçoit la DHCP REQUEST sur son interface LAN. Si l'adresse LAN-Trans indiquée est toujours allouable, le service PS DOIT alors envoyer DHCP ACK au client soit en unidiffusion soit comme diffusion sur liaison spécifique (conformément au bit BROADCAST du champ fanions de la demande DHCP REQUEST).	Approvision-nement terminé.	En cas d'échec, le client dépassera la temporisation selon le protocole DHCP et CHPSLT-1 sera répétée.
NOTE 1 – Si le client connaît l'adresse IP précédente (par exemple à la suite d'un réamorçage), il peut omettre le message DHCP DISCOVER et passer à l'étape 3. NOTE 2 – Si le client est situé dans un réseau sans diffusion, il est censé envoyer le message en unidiffusion au serveur DHCP. NOTE 3 – Si le client est situé sur un réseau sans diffusion, il est censé envoyer le message en unidiffusion au service portail.			

13.5.1 Choix d'adresse LAN-Trans et des options DHCP

Le service PS DOIT choisir l'adresse LAN-Trans qu'il offre à partir de la gamme indiquée par les variables de base MIB cabhCdpLanPoolStart et cabhCdpLanPoolEnd.

Le serveur CDS de services portail DOIT inclure dans le message DHCP OFFER les options obligatoires énumérées au Tableau 7-3.

13.6 Processus d'approvisionnement: client DHCP dans le secteur LAN-Pass

Certaines applications de réseau LAN résidentiel ne fonctionnent pas correctement avec une adresse de couche Réseau traduite. Afin de tenir compte de ces applications, le service portail est activé de façon à fonctionner en mode de traversée (dérivation transparente). Comme décrit au § 8.2.2.2, la dérivation se produit lorsque le système NMS du réseau câblé règle le mode de traitement primaire de paquet (objet cabhCapPrimaryMode) à 'traversée' ou lorsqu'il écrit les adresses MAC de dispositifs IP de réseau LAN individuels dans la table de traversée (objet cabhCapPassthroughTable). La Figure 13-7 décrit le processus de demande et d'attribution d'une adresse IP aux dispositifs IP de réseau LAN pour lesquels le service portail a été préconfiguré de façon à dériver le trafic. Lorsque le service portail a été configuré pour dériver du trafic pour un dispositif IP de réseau LAN, les messages DHCP DISCOVER et DHCP REQUEST produits par cet dispositif IP de réseau LAN seront servis par le serveur DHCP du réseau câblé et non par le serveur CDS.

Le processus d'approvisionnement pour le dispositif IP de réseau LAN situé dans le secteur LAN-Pass DOIT survenir via la séquence décrite à la Figure 13-7 et détaillé au Tableau 13-5.

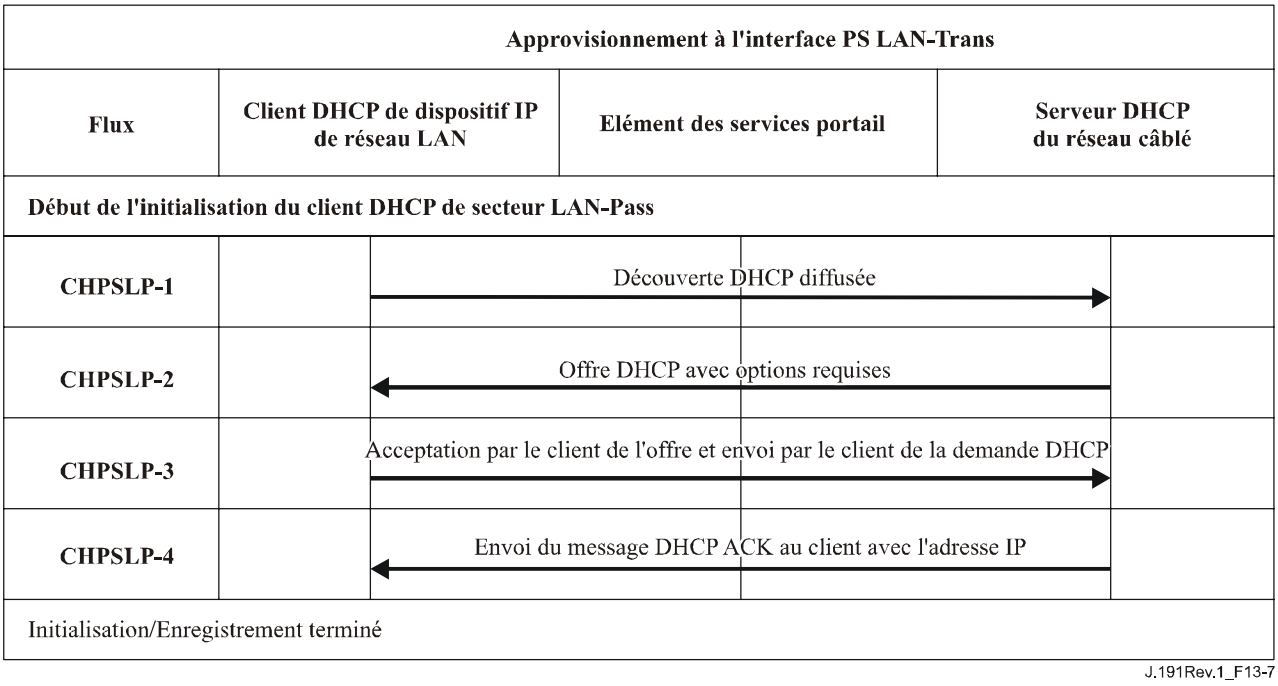


Figure 13-7/J.191 – Processus d'approvisionnement pour dispositif IP de réseau LAN situé dans le secteur LAN-Pass

Tableau 13-5/J.191 – Description des flux pour le processus d'approvisionnement du service portail par secteur LAN-Pass

Etape de flux	Approvisionnement du client d'adresse de traversée	Séquence normale	Séquence d'échec
CHPSLP-1	*Message DHCP DISCOVER en diffusion* Le dispositif IP de réseau LAN diffuse un message DHCP DISCOVER sur son réseau LAN local (Note). Le service PS reçoit le paquet DHCP DISCOVER en diffusion à son interface avec le réseau LAN et DOIT dériver le paquet de façon transparente vers l'interface WAN sans changer le contenu du paquet.	Passer à l'étape CHPSLP-2.	En cas d'échec selon le protocole DHCP, répéter CHPSLP-1.
CHPSLP-2	*Message DHCP OFFER* Le serveur DHCP situé à la tête de réseau reçoit le paquet DHCP DISCOVER et attribue une adresse IP accessible de l'extérieur avec les autres options, construit un paquet DHCP OFFER et transmet l'offre DHCP OFFER au dispositif IP de réseau LAN. Le service PS DOIT dériver de façon transparente l'offre DHCP OFFER de son interface WAN à son interface LAN sans changer le contenu du paquet IP.	Passer à l'étape CHPSLP-3.	En cas d'échec, le dispositif IP de réseau LAN dépassera la temporisation selon le protocole DHCP et CHPSLP-1 sera répétée.
CHPSLP-3	*DHCP REQUEST* Le dispositif IP de réseau LAN reçoit l'offre DHCP OFFER et produit un message DHCP REQUEST. Le service PS DOIT dériver de façon transparente la demande DHCP REQUEST de son interface LAN à son interface WAN sans changer le contenu du paquet IP.	Passer à l'étape CHPSLP-4.	En cas d'échec selon le protocole DHCP, répéter CHPSLP-1.
CHPSLP-4	*DHCP ACK* Le serveur DHCP de tête de réseau reçoit la demande DHCP REQUEST et envoie l'acquittement DHCP ACK au dispositif IP de réseau LAN avec l'adresse IPv4 du dispositif IP de réseau LAN. Le service PS DOIT dériver de façon transparente l'acquittement DHCP ACK de son interface WAN à son interface LAN sans changer le contenu du paquet IP.	Approvisionnement terminé	En cas d'échec, le dispositif IP de réseau LAN dépassera la temporisation selon le protocole DHCP et CHPSLP-1 sera répétée.
NOTE – Si le client est situé dans un réseau sans diffusion, il doit transmettre le message en unidiffusion au serveur DHCP ou à l'agent relais DHCP situé dans le réseau câblé.			

Annexe A

Objets de base MIB

La présente annexe énumère tous les objets de base MIB exigés, comme indiqué au § 6.3.7.

Nom/Paramètre de base MIB	Accès max	Entrées persistantes	Nombre d'entrées persistantes
	mib-2 système		
sysDescr	lecture seule	N/A	N/A
sysObjectID	lecture seule	N/A	N/A
sysUpTime	lecture seule	N/A	N/A
sysContact	lecture-écriture	Oui	1
sysName	lecture-écriture	Oui	1
sysLocation	lecture-écriture	Oui	1
sysServices	lecture seule	N/A	N/A
	interfaces [RFC 2863]		
ifNumber	lecture seule	N/A	N/A
ifTable/ifEntry			
ifIndex	lecture seule	N/A	N/A
ifDescr	lecture seule	N/A	N/A
ifType	lecture seule	N/A	N/A
ifMtu	lecture seule	N/A	N/A
ifSpeed	lecture seule	N/A	N/A
ifPhysAddress	lecture seule	N/A	N/A
ifAdminStatus	lecture-écriture	N/A	N/A
ifOperStatus	lecture seule	N/A	N/A
ifLastChange	lecture seule	N/A	N/A
ifInOctets	lecture seule	N/A	N/A
ifInUcastPkts	lecture seule	N/A	N/A
ifInDiscards	lecture seule	N/A	N/A
ifInErrors	lecture seule	N/A	N/A
ifInUnknownProtos	lecture seule	N/A	N/A
ifOutOctets	lecture seule	N/A	N/A
ifOutUcastPkts	lecture seule	N/A	N/A
ifOutDiscards	lecture seule	N/A	N/A
ifOutErrors	lecture seule	N/A	N/A
	ip [RFC 2011]		
ipForwarding	lecture-écriture	Non	N/A
ipDefaultTTL	lecture-écriture	Non	N/A
ipInReceives	lecture seule	N/A	N/A

Nom/Paramètre de base MIB	Accès max	Entrées persistantes	Nombre d'entrées persistantes
ipInHdrErrors	lecture seule	N/A	N/A
ipInAddrErrors	lecture seule	N/A	N/A
ipForwDatagrams	lecture seule	N/A	N/A
ipInUnknownProtos	lecture seule	N/A	N/A
ipInDiscards	lecture seule	N/A	N/A
ipInDelivers	lecture seule	N/A	N/A
ipOutRequests	lecture seule	N/A	N/A
ipOutDiscards	lecture seule	N/A	N/A
ipOutNoRoutes	lecture seule	N/A	N/A
ipReasmTimeout	lecture seule	N/A	N/A
ipReasmReqds	lecture seule	N/A	N/A
ipReasmOKs	lecture seule	N/A	N/A
ipReasmFails	lecture seule	N/A	N/A
ipFragOKs	lecture seule	N/A	N/A
ipFragFails	lecture seule	N/A	N/A
ipFragCreates	lecture seule	N/A	N/A
ipNetToMediaTable/ipNetToMediaEntry			
ipNetToMediaIfIndex	lecture-création	Non	N/A
ipNetToMediaPhyAddress	lecture-création	Non	N/A
ipNetToMediaNetAddress	lecture-création	Non	N/A
ipNetToMediaType	lecture-création	Non	N/A
	icmp		
icmpInMsgs	lecture seule	N/A	N/A
icmpInErrors	lecture seule	N/A	N/A
icmpInDestUnreachs	lecture seule	N/A	N/A
icmpInTimeExcds	lecture seule	N/A	N/A
icmpInParmProbs	lecture seule	N/A	N/A
icmpInSrcQuenchs	lecture seule	N/A	N/A
icmpInRedirects	lecture seule	N/A	N/A
icmpInEchos	lecture seule	N/A	N/A
icmpInEchosReps	lecture seule	N/A	N/A
icmpInTimestamps	lecture seule	N/A	N/A
icmpInTimestampsReps	lecture seule	N/A	N/A
icmpInAddrMasks	lecture seule	N/A	N/A
icmpInAddrMaskReps	lecture seule	N/A	N/A
icmpOutMsgs	lecture seule	N/A	N/A
icmpOutErrors	lecture seule	N/A	N/A
icmpOutDestUnreachs	lecture seule	N/A	N/A
icmpOutTimeExcds	lecture seule	N/A	N/A
icmpOutParmProbs	lecture seule	N/A	N/A

Nom/Paramètre de base MIB	Accès max	Entrées persistantes	Nombre d'entrées persistantes
icmpOutSrcQuenchs	lecture seule	N/A	N/A
icmpOutRedirects	lecture seule	N/A	N/A
icmpOutEchos	lecture seule	N/A	N/A
icmpOutEchosReps	lecture seule	N/A	N/A
icmpOutTimestamps	lecture seule	N/A	N/A
icmpOutTimestampReps	lecture seule	N/A	N/A
icmpOutAddrMasks	lecture seule	N/A	N/A
icmpOutAddrMaskReps	lecture seule	N/A	N/A
udp [RFC 2013]			
udpInDatagrams	lecture seule	N/A	N/A
udpNoPorts	lecture seule	N/A	N/A
udpInErrors	lecture seule	N/A	N/A
udpOutDatagrams	lecture seule	N/A	N/A
udpTable/udpEntry			
udpLocalAddress	lecture seule	N/A	N/A
udpLocalPort	lecture seule	N/A	N/A
transmission [draft-ietf-ipcdn-bpiplus-mib-12]			
docsIfMib			
docsBpi2MIB			
docsBpi2MIBObjects			
docsBpi2CmObjects			
docsBpi2CmCertObjects			
docsBpi2CmDeviceCertTable/docsBpi2CmDeviceCertEntry			
docsBpi2CmDeviceCmCert	lecture-écriture	Oui	5
docsBpi2CmDeviceManufCert	lecture seule	N/A	N/A
docsBpi2CodeDownloadGroup			
docsBpi2CodeDownloadStatusCode	lecture seule	N/A	N/A
docsBpi2CodeDownloadStatusString	lecture seule	N/A	N/A
docsBpi2CodeMfgOrgName	lecture seule	N/A	N/A
docsBpi2CodeMfgCodeAccessStart	lecture seule	N/A	N/A
docsBpi2CodeMfgCvcAccessStart	lecture seule	N/A	N/A
docsBpi2CodeCoSignerOrgName	lecture seule	N/A	N/A
docsBpi2CodeCoSignerCodeAccessStart	lecture seule	N/A	N/A
docsBpi2CodeCoSignerCvcAccessStart	lecture seule	N/A	N/A
docsBpi2CodeCvcUpdate	lecture-écriture	Oui	1
snmp [RFC 3416]			
snmpInPkts	lecture seule	N/A	N/A
snmpInBadVersions	lecture seule	N/A	N/A
snmpInBadCommunityNames	lecture seule	N/A	N/A
snmpInBadCommunityUses	lecture seule	N/A	N/A

Nom/Paramètre de base MIB	Accès max	Entrées persistantes	Nombre d'entrées persistantes
snmpInASNParseErrs	lecture seule	N/A	N/A
snmpEnableAuthenTraps	lecture-écriture	Non	N/A
snmpSilentDrops	lecture seule	N/A	N/A
ifMIB [RFC 2863]			
ifMIBOjects			
ifXTable/ifXEntry			
ifName	lecture seule	N/A	N/A
ifInMulticastPkts	lecture seule	N/A	N/A
ifInBroadcastPkts	lecture seule	N/A	N/A
ifOutMulticastPkts	lecture seule	N/A	N/A
ifOutBroadcastPkts	lecture seule	N/A	N/A
ifLinkUpDownTrapEnable	lecture-écriture	Non	N/A
ifHighSpeed	lecture seule	N/A	N/A
ifPromiscuousMode	lecture-écriture	N/A	N/A
ifConnectorPresent	lecture seule	N/A	N/A
ifAlias	lecture-écriture	Non	N/A
ifCounterDiscontinuityTime	lecture seule	N/A	N/A
ifStackTable/ifStackEntry			
ifStackHigherLayer	lecture seule	N/A	N/A
IfStackLowerLayer	lecture seule	N/A	N/A
ifStackStatus	lecture seule	N/A	N/A
docsDev [RFC 2669]			
docsDevMIBObjects			
docsDevNmAccessTable/docsDevNmAccessEntry			
docsDevNmAccessIndex	non accessible	N/A	N/A
docsDevNmAccessIp	lecture-création	Non	N/A
docsDevNmAccessIpMask	lecture-création	Non	N/A
docsDevNmAccessCommunity	lecture-création	Non	N/A
docsDevNmAccessControl	lecture-création	Non	N/A
docsDevNmAccessInterfaces	lecture-création	Non	N/A
docsDevNmAccessStatus	lecture-création	Non	N/A
docsDevNmAccessTrapVersion	lecture-création	Non	N/A
docsDevSoftware			
docsDevSwServer	lecture-écriture	Oui	1
docsDevSwFilename	lecture-écriture	Oui	1
docsDevSwAdminStatus	lecture-écriture	Non	1
docsDevSwOperStatus	lecture seule	N/A	N/A
docsDevSwCurrentVers	lecture seule	N/A	N/A

Nom/Paramètre de base MIB	Accès max	Entrées persistantes	Nombre d'entrées persistantes
	docsDevEvent		
docsDevEvControl	lecture-écriture	Non	N/A
docsDevEvSyslog	lecture-écriture	Non	N/A
docsDevEvThrottleAdminStatus	lecture-écriture	Non	N/A
docsDevEvThrottleInhibited	lecture seule	N/A	N/A
docsDevEvThrottleThreshold	lecture-écriture	Non	N/A
docsDevEvThrottleInterval	lecture-écriture	Non	N/A
docsDevEvControlTable/docsDevEvControlEntry			
docsDevEvPriority	non accessible	N/A	N/A
docsDevEvReporting	lecture-écriture	Non	N/A
docsDevEventTable/docsDevEventEntry			
docsDevEvIndex	non accessible	N/A	N/A
docsDevEvFirstTime	lecture seule	Oui	1
docsDevEvLastTime	lecture seule	Oui	1
docsDevEvCounts	lecture seule	Oui	1
docsDevEvLevel	lecture seule	Oui	1
docsDevEvId	lecture seule	Oui	1
docsDevEvText	lecture seule	Oui	1
	private		
	enterprises		
	cableLabs		
	clabProject		
	clabProjCableHome		
	cabhPsDevMib		
	cabhPsDevBase		
cabhPsDevDateTime	lecture-écriture	Non	N/A
cabhPsDevResetNow	lecture-écriture	Non	N/A
cabhPsDevSerialNumber	lecture seule	N/A	N/A
cabhPsDevHardwareVersion	lecture seule	N/A	N/A
cabhPsDevWanManMacAddress	lecture seule	N/A	N/A
cabhPsDevWanDataMacAddress	lecture seule	N/A	N/A
cabhPsDevTypeIdentifier	lecture seule	N/A	N/A
cabhPsDevSetToFactory	lecture-écriture	Non	N/A
cabhPsDevTodSyncStatus	lecture seule	N/A	N/A
cabhPsDevProvMode	lecture seule	N/A	N/A
cabhPsDevLastSetToFactory	lecture seule	–	N/A
	cabhPsDevProv		
cabhPsDevProvisioningTimer	lecture-écriture	Non	N/A
cabhPsDevProvConfigFile	lecture-écriture	Non	N/A
cabhPsDevProvConfigHash	lecture-écriture	Non	N/A

Nom/Paramètre de base MIB	Accès max	Entrées persistantes	Nombre d'entrées persistantes
cabhPsDevProvConfigFileSize	lecture seule	N/A	N/A
cabhPsDevProvConfigFileStatus	lecture seule	N/A	N/A
cabhPsDevProvConfigTLVProcessed	lecture seule	N/A	N/A
cabhPsDevProvConfigTLVRejected	lecture seule	N/A	N/A
cabhPsDevProvSolicitedKeyTimeout	lecture-écriture	Oui	1
cabhPsDevProvState	lecture seule	N/A	N/A
cabhPsDevProvAuthState	lecture seule	N/A	N/A
cabhPsDevTimeServerAddrType	lecture seule	N/A	N/A
cabhPsDevTimeServerAddr	lecture seule	N/A	N/A
cabhSecMib			
cabhSecFwObjects			
cabhSecFwBase			
cabhSecFwPolicyFileEnable	lecture-écriture	Non	N/A
cabhSecFwPolicyFileURL	lecture-écriture	Non	N/A
cabhSecFwPolicyFileHash	lecture-écriture	Non	N/A
cabhSecFwPolicyFileOperStatus	lecture seule	N/A	N/A
cabhSecFwPolicyFileCurrentVersion	lecture seule	N/A	N/A
cabhSecFwPolicySuccessfulFileURL, Max-Access	lecture seule	Oui	1
cabhSecFwLogCtl			
cabhSecFwEventType1Enable	lecture-écriture	Non	N/A
cabhSecFwEventType2Enable	lecture-écriture	Non	N/A
cabhSecFwEventType3Enable	lecture-écriture	Non	N/A
cabhSecFwEventAttackAlertThreshold	lecture-écriture	Non	N/A
cabhSecFwEventAttackAlertPeriod	lecture-écriture	Non	N/A
cabhSecCertObjects			
cabhSecCertPsCert	lecture seule	Oui	1
cabhCapMib			
cabhCapObjects			
cabhCapBase			
cabhCapTcpTimeWait	lecture-écriture	Oui	1
cabhCapUdpTimeWait	lecture-écriture	Oui	1
cabhCapIcmpTimeWait	lecture-écriture	Oui	1
cabhCapPrimaryMode	lecture-écriture	Non	N/A
cabhCapSetToFactory	lecture-écriture	Non	N/A
cabhCapLastSetToFactory	Lecture seule	–	N/A
cabhCapMap			
cabhCapMappingTable/cabhCapMappingEntry			
cabhCapMappingIndex	non accessible	Oui (Note)	16
cabhCapMappingWanAddrType	lecture-création	Oui (Note)	16
cabhCapMappingWanAddr	lecture-création	Oui (Note)	16

Nom/Paramètre de base MIB	Accès max	Entrées persistantes	Nombre d'entrées persistantes
cabhCapMappingWanPort	lecture-création	Oui (Note)	16
cabhCapMappingLanAddrType	lecture-création	Oui (Note)	16
cabhCapMappingLanAddr	lecture-création	Oui (Note)	16
cabhCapMappingLanPort	lecture-création	Oui (Note)	16
cabhCapMappingMethod	lecture seule	N/A	16
cabhCapMappingProtocol	lecture-création	Oui (Note)	16
cabhCapMappingRowStatus	lecture-création	Oui	16
cabhCapPass-throughTable/cabhCapPass-throughEntry			
cabhCapPass-throughIndex	non accessible	Oui	16
cabhCapPass-throughMACAddr	lecture-création	Oui	16
cabhCapPass-throughRowStatus	lecture-création	Oui	16

NOTE – Les objets cabhCapMappingEntry sont persistants s'ils sont approvisionnés par le système NMS et non persistants s'ils sont créés de façon dynamique sur la base du trafic sortant. Voir le § 8.3.2.2.

cabhCdpMib			
cabhCdpObjects			
cabhCdpBase			
cabhCdpSetToFactory	lecture-écriture	Non	N/A
cabhCdpLanTransCurCount	lecture seule	N/A	N/A
cabhCdpLanTransThreshold	lecture-écriture	Non	N/A
cabhCdpLanTransAction	lecture-écriture	Non	N/A
cabhCdpWanDataIpAddrCount	lecture-écriture	Non	N/A
cabhCdpLastSetToFactory	lecture seule	–	N/A
cabhCdpAddr			
cabhCdpLanAddrTable/cabhCdpLanAddrEntry			
cabhCdpLanAddrIpType	non accessible	Oui	16
cabhCdpLanAddrIp	non accessible	Oui	16
cabhCdpLanAddrClientID	lecture-création	Oui	16
cabhCdpLanAddrLeaseCreateTime	lecture seule	Oui	16
cabhCdpLanAddrLeaseExpireTime	lecture seule	Oui	16
cabhCdpLanAddrMethod	lecture seule	Oui	16
cabhCdpLanAddrHostName	lecture seule	Oui	16
cabhCdpLanAddrRowStatus	lecture-création	Oui	16
cabhCdpWanDataAddrTable/cabhCdpWanDataAddrEntry			
cabhCdpWanDataAddrIndex	non accessible	N/A	N/A
cabhCdpWanDataAddrClientId	lecture-création	Non	N/A
cabhCdpWanDataAddrIpType	lecture seule	N/A	N/A
cabhCdpWanDataAddrIp	lecture seule	N/A	N/A
cabhCdpWanDataAddrRenewalTime	lecture seule	N/A	N/A
cabhCdpWanDataAddrRowStatus	lecture-création	Non	N/A
cabhCdpWanDataAddrServerTable/cabhCdpWanDataAddrServerEntry			
cabhCdpWanDataAddrDnsIpType	non accessible	N/A	N/A

Nom/Paramètre de base MIB	Accès max	Entrées persistantes	Nombre d'entrées persistantes
cabhCdpWanDataAddrDnsIp	non accessible	N/A	N/A
cabhCdpWanDataAddrDnsRowStatus	lecture-création	Non	N/A
	cabhCdpServer		
cabhCdpLanPoolStartType	lecture-écriture	Oui	1
cabhCdpLanPoolStart	lecture-écriture	Oui	1
cabhCdpLanPoolEndType	lecture-écriture	Oui	1
cabhCdpLanPoolEnd	lecture-écriture	Oui	1
cabhCdpServerNetworkNumberType	lecture-écriture	Oui	1
cabhCdpServerNetworkNumber	lecture-écriture	Oui	1
cabhCdpServerSubnetMaskType	lecture-écriture	Oui	1
cabhCdpServerSubnetMask	lecture-écriture	Oui	1
cabhCdpServerTimeOffset	lecture-écriture	Oui	1
cabhCdpServerRouterType	lecture-écriture	Oui	1
cabhCdpServerRouter	lecture-écriture	Oui	1
cabhCdpServerDnsAddressType	lecture-écriture	Oui	1
cabhCdpServerDnsAddress	lecture-écriture	Oui	1
cabhCdpServerSyslogAddressType	lecture-écriture	Oui	1
cabhCdpServerSyslogAddress	lecture-écriture	Oui	1
cabhCdpServerDomainName	lecture-écriture	Oui	1
cabhCdpServerTTL	lecture-écriture	Oui	1
cabhCdpServerInterfaceMTU	lecture-écriture	Oui	1
cabhCdpServerVendorSpecific	lecture-écriture	Oui	1
cabhCdpServerLeaseTime	lecture-écriture	Oui	1
cabhCdpServerDhcpAddressType	lecture-écriture	Oui	1
cabhCdpServerDhcpAddress	lecture-écriture	Oui	1
cabhCdpServerControl	lecture-écriture	Non	N/A
cabhCdpServerCommitStatus	lecture seule	–	N/A
	cabhCtpMib		
	cabhCtpObjects		
	cabhCtpBase		
cabhCtpSetToFactory	lecture-écriture	Non	N/A
cabhCtpLastSetToFactory	lecture seule	–	N/A
	cabhCtpConnSpeed		
cabhCtpConnSrcIpType	lecture-écriture	Non	N/A
cabhCtpConnSrcIp	lecture-écriture	Non	N/A
cabhCtpConnDestIpType	lecture-écriture	Non	N/A
cabhCtpConnDestIp	lecture-écriture	Non	N/A
cabhCtpConnProto	lecture-écriture	Non	N/A
cabhCtpConnNumPkts	lecture-écriture	Non	N/A
cabhCtpConnPktSize	lecture-écriture	Non	N/A

Nom/Paramètre de base MIB	Accès max	Entrées persistantes	Nombre d'entrées persistantes
cabhCtpConnTimeOut	lecture-écriture	Non	N/A
cabhCtpConnControl	lecture-écriture	Non	N/A
cabhCtpConnStatus	lecture seule	N/A	N/A
cabhCtpConnPktsSent	lecture seule	N/A	N/A
cabhCtpConnPktsRecv	lecture seule	N/A	N/A
cabhCtpConnRTT	lecture seule	N/A	N/A
cabhCtpConnThroughput	lecture seule	N/A	N/A
cabhCtpPing			
cabhCtpPingSrcIpType	lecture-écriture	Non	N/A
cabhCtpPingSrcIp	lecture-écriture	Non	N/A
cabhCtpPingDestIpType	lecture-écriture	Non	N/A
cabhCtpPingDestIp	lecture-écriture	Non	N/A
cabhCtpPingNumPkts	lecture-écriture	Non	N/A
cabhCtpPingPktSize	lecture-écriture	Non	N/A
cabhCtpPingTimeBetween	lecture-écriture	Non	N/A
cabhCtpPingTimeOut	lecture-écriture	Non	N/A
cabhCtpPingControl	lecture-écriture	Non	N/A
cabhCtpPingStatus	lecture seule	N/A	N/A
cabhCtpPingNumSent	lecture seule	N/A	N/A
cabhCtpPingNumRecv	lecture seule	N/A	N/A
cabhCtpPingAvgRTT	lecture seule	N/A	N/A
cabhCtpPingMinRTT	lecture seule	N/A	N/A
cabhCtpPingMaxRTT	lecture seule	N/A	N/A
cabhCtpPingNumIcmpError	lecture seule	N/A	N/A
cabhCtpPingIcmpError	lecture seule	N/A	N/A
experimental			
snmpUSMDHObjectsMIB [RFC 2786]			
usmDHKeyObjects			
usmDHPublicObjects			
usmDHPParamaters	lecture-écriture	Non	N/A
usmDHUserKeyTable/usmDHUserKeyEntry			
usmDHUserAuthKeyChange	lecture-création	Non	N/A
usmDHUserOwnAuthKeyChange	lecture-création	Non	N/A
usmDHUserPrivKeyChange	lecture-création	Non	N/A
usmDHUserOwnPrivKeyChange	lecture-création	Non	N/A
usmDHKickstartGroup			
usmDHKickstartTable/usmDHKickstartEntry			
usmDHKickstartIndex	non accessible	Non	N/A
usmDHKickstartMyPublic	lecture seule	N/A	N/A

Nom/Paramètre de base MIB	Accès max	Entrées persistantes	Nombre d'entrées persistantes
usmDHKickstartMgrPublic	lecture seule	N/A	N/A
usmDHKickstartSecurityName	lecture seule	N/A	N/A
snmpV2			
snmpModules			
snmpMIB			
snmpMIBObjects			
snmpSet			
snmpSetSerialNo	lecture-écriture	Non	N/A
snmpFrameworkMIB [RFC 2576]			
snmpEngine			
snmpEngineID	lecture seule	N/A	N/A
snmpEngineBoots	lecture seule	Oui	1
snmpEngineTime	lecture seule	N/A	N/A
snmpEngineMaxMessageSize	lecture seule	N/A	N/A
snmpMPDMIB [RFC 3412]			
snmpMPDObjects			
snmpMPDStats			
snmpUnknownSecurityModels	lecture seule	N/A	N/A
snmpInvalidMsgs	lecture seule	N/A	N/A
snmpUnknownPDUHandlers	lecture seule	N/A	N/A
snmpTargetMIB [RFC 3413]			
snmpTargetObjects			
snmpTargetSpinLock	lecture-écriture	Non	N/A
snmpTargetAddrTable/snmpTargetAddrEntry			
snmpTargetAddrName	non accessible	Non	N/A
snmpTargetAddrTDomain	lecture-création	Non	N/A
snmpTargetAddrTAddress	lecture-création	Non	N/A
snmpTargetAddrTimeout	lecture-création	Non	N/A
snmpTargetAddrRetryCount	lecture-création	Non	N/A
snmpTargetAddrTagList	lecture-création	Non	N/A
snmpTargetAddrParams	lecture-création	Non	N/A
snmpTargetAddrStorageType	lecture-création	Non	N/A
snmpTargetAddrRowStatus	lecture-création	Non	N/A
snmpTargetParamsTable/snmpTargetParamsEntry			
snmpTargetParamsName	non accessible	Non	N/A
snmpTargetParamsMPModel	lecture-création	Non	N/A
snmpTargetParamsSecurityModel	lecture-création	Non	N/A
snmpTargetParamsSecurityName	lecture-création	Non	N/A
snmpTargetParamsSecurityLevel	lecture-création	Non	N/A

Nom/Paramètre de base MIB	Accès max	Entrées persistantes	Nombre d'entrées persistantes
snmpTargetParamsStorageType	lecture-création	Non	N/A
snmpTargetParamsRowStatus	lecture-création	Non	N/A
snmpUnavailableContexts	lecture seule	N/A	N/A
snmpUnknownContexts	lecture seule	N/A	N/A
snmpNotificationMIB [RFC 3413]			
snmpNotifyObjects			
snmpNotifyTable/snmpNotifyEntry			
snmpNotifyName	non accessible	Non	N/A
snmpNotifyTag	lecture-création	Non	N/A
snmpNotifyType	lecture-création	Non	N/A
snmpNotifyStorageType	lecture-création	Non	N/A
snmpNotifyRowStatus	lecture-création	Non	N/A
snmpNotifyFilterProfileTable/snmpNotifyFilterProfileEntry			
snmpNotifyFilterProfileName	lecture-création	Non	N/A
snmpNotifyFilterProfileStorType	lecture-création	Non	N/A
snmpNotifyFilterProfileRowStatus	lecture-création	Non	N/A
snmpNotifyFilterTable/snmpNotifyFilterEntry			
snmpNotifyFilterSubtree	non accessible	Non	N/A
snmpNotifyFilterMask	lecture-création	Non	N/A
snmpNotifyFilterType	lecture-création	Non	N/A
snmpNotifyFilterStorageType	lecture-création	Non	N/A
snmpNotifyFilterRowStatus	lecture-création	Non	N/A
snmpUsmMIB [RFC 3414]			
usmStats			
usmStatsUnsupportedSecLevels	lecture seule	N/A	N/A
usmStatsNotInTimeWindows	lecture seule	N/A	N/A
usmStatsUnknownUserNames	lecture seule	N/A	N/A
usmStatsUnknownEngineIDs	lecture seule	N/A	N/A
usmStatsWrongDigests	lecture seule	N/A	N/A
usmStatsDecryptionErrors	lecture seule	N/A	N/A
usmUser			
usmUserSpinLock	lecture-écriture	Non	N/A
usmUserTable/usmUserEntry			
usmUserEngineID	non accessible	N/A	N/A
usmUserName	non accessible	N/A	N/A
usmUserSecurityName	lecture seule	N/A	N/A
usmUserCloneFrom	lecture-création	Non	N/A
usmUserAuthProtocol	lecture-création	Non	N/A
usmUserAuthKeyChange	lecture-création	Non	N/A
usmUserOwnAuthKeyChange	lecture-création	Non	N/A

Nom/Paramètre de base MIB	Accès max	Entrées persistantes	Nombre d'entrées persistantes
usmUserPrivProtocol	lecture-création	Non	N/A
usmUserPrivKeyChange	lecture-création	Non	N/A
usmUserOwnPrivKeyChange	lecture-création	Non	N/A
usmUserPublic	lecture-création	Non	N/A
usmUserStorageType	lecture-création	Non	N/A
usmUserStatus	lecture-création	Non	N/A
SNMP-VIEW-BASED-ACM-MIB [RFC 3415]			
snmpVacmMIB			
vacmMIBObjects			
vacmContextTable/vacmContextEntry			
vacmContextName	lecture seule	Non	N/A
vacmSecurityToGroupTable/vacmSecurityToGroupEntry			
vacmSecurityModel	non accessible	Non	N/A
vacmSecurityName	non accessible	Non	N/A
vacmGroupName	lecture-création	Non	N/A
vacmSecurityToGroupStorageType	lecture-création	Non	N/A
vacmSecurityToGroupStatus	lecture-création	Non	N/A
vacmAccessTable/vacmAccessEntry			
vacmAccessContextPrefix	non accessible	Non	N/A
vacmAccessSecurityModel	non accessible	Non	N/A
vacmAccessSecurityLevel	non accessible	Non	N/A
vacmAccessContextMatch	lecture-création	Non	N/A
vacmAccessReadViewName	lecture-création	Non	N/A
vacmAccessWriteViewName	lecture-création	Non	N/A
vacmAccessNotifyViewName	lecture-création	Non	N/A
vacmAccessStorageType	lecture-création	Non	N/A
vacmAccessStatus	lecture-création	Non	N/A
vacmMIBViews			
vacmViewSpinLock	lecture-écriture	Non	N/A
vacmViewTreeFamilyTable/vacmViewTreeFamilyEntry			
vacmViewTreeFamilyViewName	non accessible	Non	N/A
vacmViewTreeFamilySubtree	non accessible	Non	N/A
vacmViewTreeFamilyMask	lecture-création	Non	N/A
vacmViewTreeFamilyType	lecture-création	Non	N/A
vacmViewTreeFamilyStorageType	lecture-création	Non	N/A
vacmViewTreeFamilyStatus	lecture-création	Non	N/A

Nom/Paramètre de base MIB	Accès max	Entrées persistantes	Nombre d'entrées persistantes
snmpCommunityMIB [RFC 2576]			
snmpCommunityMIBObjects			
snmpCommunityTable/snmpCommunityEntry			
snmpCommunityIndex	non accessible	Non	N/A
snmpCommunityName	lecture-création	Non	N/A
snmpCommunitySecurityName	lecture-création	Non	N/A
snmpCommunityContextEngineID	lecture-création	Non	N/A
snmpCommunityContextName	lecture-création	Non	N/A
snmpCommunityTransportTag	lecture-création	Non	N/A
snmpCommunityStorageType	lecture-création	Non	N/A
snmpCommunityStatus	lecture-création	Non	N/A
snmpTargetAddrExtTable/snmpTargetAddrExtEntry			
snmpTargetAddrTMask	lecture-création	Non	N/A
snmpTargetAddrMMS	lecture-création	Non	N/A
clabSecCertObject			
clabSrvcPrvdrRootCACert	lecture seule	N/A	N/A
clabCVCRootCACert	lecture seule	N/A	N/A
clabCVCCACert	lecture seule	N/A	N/A
clabMfgCVCCert	lecture seule	N/A	N/A

Annexe B

Format et contenu des événements, de l'enregistrement SYSLOG et des transferts TRAP du protocole SNMP

Le Tableau B.1 résume les formats et contenus des entrées d'événements d'enregistrement local, des messages syslog et des transferts SNMP.

Chaque rangée du Tableau B.1 spécifie un événement que le service portail doit être capable de générer. Le service portail doit signaler ces événements par l'un des trois moyens suivants ou par les trois: enregistrement d'événement local comme effectué par le tableau d'événement local du document RFC 2669, SYSLOG, et transfert SNMP. Le format SYSLOG est spécifié au § 6.5.1.3 et le format de transfert SNMP est défini dans la présente annexe, à la suite du Tableau B.1.

Les deux premières colonnes indiquent à quel stade survient l'événement. La troisième colonne indique la priorité attribuée à l'événement. Ces priorités sont celles qui sont rapportées dans l'objet docsDevEvLevel dans RFC 2669 et dans le champ LEVEL (*niveau*) d'un message SYSLOG.

La quatrième colonne spécifie le texte de l'événement, qui est rapporté dans l'objet docsDevEvText du document RFC 2669 et dans le champ de texte d'un message syslog. La cinquième colonne donne des informations supplémentaires sur le texte d'événement de la quatrième colonne. Par exemple, certains des champs de texte d'événement sont constants alors que d'autres incluent des informations variables. Certaines des variables ne sont exigées que dans le journal syslog, comme décrit dans la cinquième colonne. La sixième colonne spécifie la mise à jour du code d'erreur.

La septième colonne indique un numéro d'identification unique pour l'événement, qui est attribué à l'objet docsDevEvId et au champ <eventId> d'un message syslog. La huitième colonne spécifie le transfert SNMP, qui notifie cet événement à un récepteur d'événements SNMP.

Les règles permettant de générer de façon univoque un identificateur d'événement à partir du code d'erreur sont décrites au § 6.5.1.3. Les identificateurs d'événement figurant dans le Tableau B.1 sont en format décimal.

Pour mieux illustrer le Tableau B.1, voici un exemple utilisant la première rangée dans la section événements de mise à jour logicielles.

Les deux premières colonnes sont "Mise à jour logicielle" et "Initialisation de mise à jour logicielle". La priorité d'événement est "Remarque" (*Notice*). Le texte de l'événement est "Initialiser le téléchargement de logiciel – Via NMS". La cinquième colonne indique "Pour SYSLOG seulement, ajouter: MAC addr: <P1> P1 = Adresse de commande MAC des services PS". Il s'agit d'une note sur le journal syslog. C'est-à-dire que le corps du texte d'enregistrement syslog sera quelque chose comme "Initialiser le téléchargement du logiciel – Via NMS – MAC addr: x1 x2 x3 x4 x5 x6".

La dernière colonne "Nom du transfert" correspond à l'objet cabhPsDevSwUpgradeInitTrap, dont le format est donné à la fin de la présente annexe.

Tableau B.1/J.191 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Mise à jour du code d'erreur	Identificateur d'événement	Nom du transfert
Erreurs DHCP avant l'achèvement de l'approvisionnement							
Initialiser	DHCP	Critique	Echec DHCP – Flux discover envoyé, pas d'offre reçue		D01.0	68000100	
Initialiser	DHCP	Critique	Echec DHCP – Demande envoyée, pas de réponse		D02.0	68000200	
Initialiser	DHCP	Critique	Echec DHCP – Info demandée non prise en charge		D03.0	68000300	
Initialiser	DHCP	Critique	Erreur DHCP – La réponse ne contient pas TOUS les champs valides OU le service PS n'arrive pas à déterminer le mode d'approvisionnement		D03.1	68000301	
Erreurs d'heure avant l'achèvement de l'approvisionnement							
Initialiser	HEURE	Avertissement	Demande d'heure envoyée – Pas de réponse reçue		D04.1	68000401	
Initialiser	HEURE	Avertissement	Réponse d'heure reçue – Format de données non valide		D04.2	68000402	
Erreurs TFTP avant l'achèvement de l'approvisionnement							
Initialiser	TFTP	Critique	Echec TFTP – Demande envoyée – Pas de réponse		D05.0	68000500	

Tableau B.1/J.191 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Mise à jour du code d'erreur	Identificateur d'événement	Nom du transfert
Initialiser	TFTP	Critique	Echec TFTP – Fichier de configuration PS introuvable	Pour SYSLOG seulement, ajouter: nom de fichier = <P1> P1 = nom de fichier demandé	D06.0	68000600	
Initialiser	TFTP	Critique	Echec TFTP – Paquets en désordre		D07.0	68000700	
Initialiser	TFTP	Critique	Fichier TFTP terminé mais échec du contrôle de hachage SHA-1	Pour SYSLOG seulement, ajouter: nom de fichier = <P1> P1 = nom du fichier TFTP	D08.0	68000800	
Initialiser	TFTP	Critique	Echec TFTP – Nombre maximal d'essais dépassé	Pour SYSLOG seul, ajouter: limite d'essais = <P1> P1 = nombre maximal d'essais	D09.0	68000900	
TFTP réussi							
Initialiser	TFTP	Remarque	TFTP réussi		D10.0	68001000	
Analyse grammaticale de TLV							
Initialiser	Analyse de TLV	Remarque	TLV-28 – OID non reconnu		I401.0	73040100	cabhPsDevInitTLVUnknownTrap
Initialiser	Analyse de TLV	Remarque	TLV inconnu <P1>	Pour SYSLOG seulement: <P1> = le nuplet TLV complet en hexadécimal	I401.1	73040101	cabhPsDevInitTLVUnknownTrap
Initialiser	Analyse de TLV	Remarque	Format/contenu de TLV non valide <P1>	Pour SYSLOG seulement, <P1> = le nuplet TLV complet en hexadécimal	I401.2	73040102	
Approvisionnement							
Initialiser	SNMP INFORM	Remarque	SNMP Inform a envoyé le signal de fin d'approvision. (réussite/échec)	Pour SYSLOG seulement, ajouter MAC Addr: <P1>. P1 = adresse de commande MAC des services PS	I11.0	73001100	cabhPsDevInitTrap
Initialiser	Retransmission de SNMP INFORM	Critique	SNMP Inform a envoyé le signal de fin d'approvision. (réussite/échec), pas de réponse. Renvoi du message SNMP Inform	Pour SYSLOG seulement, ajouter: MAC Addr: <P1>. P1 = adresse de commande MAC des services PS	I11.1	73001101	cabhPsDevInitRetryTrap

Tableau B.1/J.191 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Mise à jour du code d'erreur	Identificateur d'événement	Nom du transfert
SW upgrade init (initialisation de mise à jour logicielle) (Note)							
Mise à jour logicielle	Initialisation de mise à jour logicielle	Remarque	Initialiser le téléchargement du logiciel – Via NMS	Pour SYSLOG seulement, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E101.0	69010100	cabhPsDev SwUpgrade InitTrap
Mise à jour logicielle	Initialisation de mise à jour logicielle	Remarque	Initialiser le téléchargement du logiciel – Via fichier de configuration PS <P1>	P1 = nom du fichier de configuration PS du câblo-modem Pour SYSLOG seulement, ajouter: fichier logiciel: <P2> – serveur logiciel: < P3>. P2 = nom de fichier logiciel et P3 = adresse IP de serveur TFTP	E102.0	69010200	cabhPsDev SwUpgrade InitTrap
Echec général de mise à jour logicielle (Note)							
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	La mise à jour logicielle a échoué pendant le téléchargement – Maximum d'essais dépassé (3)	Pour SYSLOG seulement, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E103.0	69010300	cabhPsDev SwUpgrade FailTrap
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	La mise à jour logicielle a échoué avant le téléchargement – Pas de serveur présent	Pour SYSLOG seulement, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E104.0	69010400	cabhPsDev SwUpgrade FailTrap
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	La mise à jour logicielle a échoué avant le téléchargement – Pas de fichier présent	Pour SYSLOG seulement, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E105.0	69010500	cabhPsDev SwUpgrade FailTrap

Tableau B.1/J.191 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Mise à jour du code d'erreur	Identificateur d'événement	Nom du transfert
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	La mise à jour logicielle a échoué avant le téléchargement – Nombre maximal d'essais TFTP dépassé	Pour SYSLOG seulement, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E106.0	69010600	cabhPsDev SwUpgrade FailTrap
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	La mise à jour logicielle a échoué après le téléchargement – Fichier logiciel incompatible	Pour SYSLOG seulement, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E107.0	69010700	cabhPsDev SwUpgrade FailTrap
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	La mise à jour logicielle a échoué après le téléchargement – Fichier logiciel endommagé	Pour SYSLOG seulement, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E108.0	69010800	cabhPsDev SwUpgrade FailTrap
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Transfert pendant le téléchargement du logiciel – Panne de courant	Pour SYSLOG seulement, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E109.0	69010900	cabhPsDev SwUpgrade FailTrap
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Transfert pendant le téléchargement du logiciel – Panne radioélectrique	Pour SYSLOG seulement, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E110.0	69011000	cabhPsDev SwUpgrade FailTrap

Tableau B.1/J.191 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Mise à jour du code d'erreur	Identificateur d'événement	Nom du transfert
Réussite de mise à jour logicielle (Note)							
Mise à jour logicielle	Réussite de mise à jour logicielle	Remarque	Téléchargement du logiciel réussi – Via le système NMS	Pour SYSLOG seulement, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E111.0	69011100	cabhPsDev SwUpgrade SuccessTrap
Mise à jour logicielle	Réussite de mise à jour logicielle	Remarque	Téléchargement du logiciel réussi – Via le fichier de configuration	Pour SYSLOG seulement, ajouter: fichier logiciel: <P1> – serveur logiciel: < P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E112.0	69011200	cabhPsDev SwUpgrade SuccessTrap
Echec DHCP après l'achèvement de l'approvisionnement					D100.0	68010000	
DHCP		Erreur	DHCP RENEW envoyé – Non réponse		D101.0	68010100	cabhPsDev DHCPFail Trap
DHCP		Erreur	DHCP REBIND envoyé – Non réponse		D102.0	68010200	cabhPsDev DHCPFail Trap
DHCP		Erreur	DHCP RENEW envoyé – Option DHCP non valide		D103.0	68010300	cabhPsDev DHCPFail Trap
DHCP		Erreur	DHCP REBIND envoyé – Option DHCP non valide		D104.0	68010400	cabhPsDev DHCPFail Trap
Echec de l'heure après achèvement de l'approvisionnement							
Heure	Heure	Avertissement	Demande d'heure envoyée – Pas de réponse reçue		D04.3	68000403	cabhPsDev ToDFailTrap
Heure	Heure	Avertissement	Réponse d'heure reçue – Format de données non valide		D04.4	68000404	cabhPsDev ToDFailTrap
Vérification de fichier de code					E200		
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Contrôles de fichier de code impropres	Pour SYSLOG seulement, ajouter: fichier de code: <P1> – serveur de fichier de code: <P2>. P1 = nom de fichier de code, P2 = adresse IP du serveur de fichier de code	E201.0	69020100	cabhPsDev SwUpgrade FailTrap

Tableau B.1/J.191 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Mise à jour du code d'erreur	Identificateur d'événement	Nom du transfert
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Echec de validation de certificat CVC de constructeur	Pour SYSLOG seulement, ajouter: fichier de code: <P1> – serveur de fichier de code: <P2>. P1 = nom de fichier de code, P2 = adresse IP du serveur de fichier de code	E202.0	69020200	cabhPsDev SwUpgrade FailTrap
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Echec de validation de signature CVS de constructeur de fichier de code	Pour SYSLOG seulement, ajouter: fichier de code: <P1> – serveur de fichier de code: <P2>. P1 = nom de fichier de code, P2 = adresse IP du serveur de fichier de code	E203.0	69020300	cabhPsDev SwUpgrade FailTrap
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Echec de validation de certificat CVC de cosignataire de fichier de code	Pour SYSLOG seulement, ajouter: fichier de code: <P1> – serveur de fichier de code: <P2>. P1 = nom de fichier de code, P2 = adresse IP du serveur de fichier de code	E204.0	69020400	cabhPsDev SwUpgrade FailTrap
Mise à jour logicielle	Echec général de mise à jour logicielle	Erreur	Echec de validation de signature CVS de cosignataire de fichier de code	Pour SYSLOG seulement, ajouter: fichier de code: <P1> – serveur de fichier de code: <P2>. P1 = nom de fichier de code, P2 = adresse IP du serveur de fichier de code	E205.0	69020500	cabhPsDev SwUpgrade FailTrap
Vérification de certificat CVC							
Mise à jour logicielle	Vérification de CVC	Erreur	Format de certificat CVC de fichier de configuration impropre – Serveur TFTP: <P1> – Fichier de configuration: <P2>	P1 = adresse IP de serveur TFTP P2 = Nom de fichier de configuration	E206.0	69020600	cabhPsDev SwUpgrade CVCFailTrap

Tableau B.1/J.191 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Mise à jour du code d'erreur	Identificateur d'événement	Nom du transfert
Mise à jour logicielle	Vérification de CVC	Erreur	Echec de validation de certificat CVC de fichier de configuration – Serveur TFTP: <P1> – Fichier de configuration: <P2>	P1 = adresse IP de serveur TFTP P2 = Nom de fichier de configuration	E207.0	69020700	cabhPsDev SwUpgrade CVCFailTrap
Mise à jour logicielle	Vérification de CVC	Erreur	Format de certificat CVC par protocole SNMP impropre – Gestionnaire SNMP: <P1>	P1 = adresse IP du gestionnaire SNMP	E208.0	69020800	cabhPsDev SwUpgrade CVC FailTrap
Mise à jour logicielle	Vérification de CVC	Erreur	Echec de validation de certificat CVC par protocole SNMP – Gestionnaire SNMP: <P1>	P1 = adresse IP du gestionnaire SNMP	E209.0	69020900	cabhPsDev SwUpgrade CVCFailTrap
Evénements de portail CDP							
CDP	CDS	Remarque	Tentative d'attribution de plus d'adresses IP de réseau LAN TRANS qu'autorisé		P01.0	80000100	cabhPsDev CDPThreshold Trap
CDP	CDS	Remarque	Incapacité à obtenir toutes les adresses IP de réseau WAN-Data que le service PS a été configuré de façon à obtenir		P02.0	80000200	cabhPsDev CdpWanData IpTrap
CDP	CDS	Remarque	Incapacité à approvisionner le client LAN DHCP – réserve d'adresse IP épuisée		P03.0	80000300	cabhPsDev CdpLanIp PoolTrap
Evénements de portail CSP							
CSP	Pare-feu	Remarque	Seuil de piratage de pare-feu de type 1 et type 2 dépassé		P101.0	80010100	cabhPsDev CSPTrap
CSP	Pare-feu	Remarque	Evénement de pare-feu de type 1 détecté	P1 = adresse IP de source, P2 = adresse IP de destination, P3 = type de protocole, P4 = nom de fichier d'ensemble actif de règles, P5 = description d'événement	P102.0	80010200	cabhPsDev CSPTrap

Tableau B.1/J.191 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Mise à jour du code d'erreur	Identificateur d'événement	Nom du transfert
CSP	Pare-feu	Remarque	Evénement de pare-feu de type 2 détecté	P1 = adresse IP de source, P2 = adresse IP de destination, P3 = type de protocole, P4 = nom de fichier d'ensemble actif de règles, P5 = description d'événement	P103.0	80010300	cabhPsDev CSPTrap
CSP	Pare-feu	Remarque	La configuration de pare-feu a changé	P1 = description du changement dans les paramètres de configuration du pare-feu	P120.0	80012000	cabhPsDev CSPTrap
CSP	TFTP du pare-feu	Critique	Le téléchargement par TFTP du fichier de politique de pare-feu a échoué: demande envoyée, sans réponse	P1 = URL du fichier de politique de pare-feu demandé	P130.0	80013000	cabhPsDev CSPTrap
CSP	TFTP du pare-feu	Critique	Echec du téléchargement par TFTP du fichier de politique de pare-feu: fichier non trouvé	P1 = URL du fichier de politique de pare-feu demandé	P131.0	80013100	cabhPsDev CSPTrap
CSP	TFTP du pare-feu	Critique	Echec du téléchargement par TFTP du fichier de politique de pare-feu: fichier non valide	P1 = URL du fichier de politique de pare-feu demandé	P132.0	80013200	cabhPsDev CSPTrap
CSP	TFTP du pare-feu	Critique	Téléchargement du fichier de politique de pare-feu effectué mais échec du contrôle de hachage SHA-1	P1 = URL du fichier de politique de pare-feu demandé, P2 = valeur de hachage du fichier de politique de pare-feu	P133.0	80013300	cabhPsDev CSPTrap
CSP	TFTP du pare-feu	Critique	Le téléchargement du fichier de politique de pare-feu a dépassé le nombre maximal admissible d'essais de transfert TFTP	P1 = URL du fichier de politique de pare-feu demandé	P134.0	80013400	cabhPsDev CSPTrap

Tableau B.1/J.191 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Mise à jour du code d'erreur	Identificateur d'événement	Nom du transfert
CSP	TFTP du pare-feu	Remarque	Succès du téléchargement par TFTP du fichier de politique de pare-feu	P1 = URL du fichier de politique de pare-feu demandé Pour SYSLOG seulement, ajouter: nombre limite d'essais = <P2> P2 = nombre maximal admissible d'essais successifs	P135.0	80013500	cabhPsDev CSPTrap
Evénements de portail CAP							
CAP	C-NAT	Remarque	CAP incapable d'effectuer le mappage C-NAT. Pas d'adresse IP WAN-data disponible		P201.0	80020100	cabhPsDev CAPTrap
CAP	C-NAPT	Remarque	CAP incapable d'effectuer le mappage C-NAPT. Pas d'adresse IP WAN disponible		P250.0	80025000	cabhPsDev CAPTrap
Evénements de portail CTP							
CTP	Utilitaire de vitesse de connexion	Remarque	Succès de l'essai par utilitaire de vitesse de connexion	P1 = adresse IP de l'origine P2 = adresse IP de la destination P3 = protocole P4 = débit utile	P301.0	80030100	cabhPsDevCtp Trap
CTP	Utilitaire de vitesse de connexion	Remarque	Expiration de la temporisation de l'essai par utilitaire de vitesse de connexion	P1 = adresse IP de l'origine P2 = adresse IP de la destination P3 = protocole P4 = valeur du temporisateur (en millisecondes)	P302.0	80030200	cabhPsDevCtp Trap
CTP	Utilitaire de vitesse de connexion	Remarque	Abandon de l'essai par utilitaire de vitesse de connexion	P1 = adresse IP de l'origine P2 = adresse IP de la destination P3 = protocole P4 = valeur du temporisateur (en millisecondes)	P303.0	80030300	cabhPsDevCtp Trap

Tableau B.1/J.191 – Evénements définis pour IPCable2Home

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Mise à jour du code d'erreur	Identificateur d'événement	Nom du transfert
CTP	Utilitaire de validation par écho	Remarque	Essai de validation par écho effectué correctement	P1 = adresse IP de l'origine P2 = adresse IP de la destination P3 = temps moyen d'aller-retour	P320.0	80032000	cabhPsDevCtpTrap
CTP	Utilitaire de validation par écho	Remarque	Expiration de la temporisation de l'essai de validation par écho	P1 = adresse IP de l'origine P2 = adresse IP de la destination P3 = nombre de requêtes envoyées P4 = nombre de réponses reçues	P321.0	80032100	cabhPsDevCtpTrap
CTP	Utilitaire de validation par écho	Remarque	Abandon de l'essai de validation par écho	P1 = adresse IP de l'origine P2 = adresse IP de la destination P3 = nombre de requêtes envoyées P4 = nombre de réponses reçues	P322.0	80032200	cabhPsDevCtpTrap
NOTE – Les événements de mise à jour logicielle (téléchargement de logiciel sécurisé) ne s'appliquent qu'aux services portail autonome. Dans un service PS imbriqué, la mise à jour logicielle est commandée par le câblo-modem, de sorte que la signalisation des événements de mise à jour logicielle est gérée par le câblo-modem dans un service PS imbriqué. Voir de plus amples informations au § 11.3.7.1.							

B.1 Description des transferts automatiques

Tous les transferts spécifiés par le modèle IPCable2Home sont définis dans la spécification de base MIB de dispositif PSDev du service PS [Voir E.1].

Annexe C

Dangers et mesures préventives

C.1 Dangers

Lors du développement d'une technique de sécurité, il est important de comprendre ce que sont les principales menaces pour une application ou un environnement donné. Ces informations peuvent alors être utilisées pour choisir les utilitaires de sécurité et les technologies les plus efficaces pour la protection et la prévention contre les attaques qualifiées.

On a identifié les principaux dangers suivants pour les abonnés et les opérateurs de réseau du domicile:

C.1.1 vol de service: le vol de service se produit sous deux formes: l'accès non autorisé aux services par câble et la duplication non autorisée du contenu des services.

L'accès non autorisé implique un abonné ou une tierce partie (comme un voisin) ayant accès aux services par câble pour lesquels ils n'ont pas payé. Les dispositifs peuvent être "clonés" ou modifiés de façon à apparaître comme des dispositifs qualifiés au domicile de l'abonné. Cela peut aussi dégrader les performances de fourniture du service car ces dispositifs consomment des ressources de transport supplémentaires sur le câble HFC et dans les réseaux du domicile.

La duplication non autorisée implique habituellement un abonné ou une tierce partie (comme un voisin) qui fait des copies illégales du contenu du service. Dans certains cas, ces copies sont distribuées à d'autres consommateurs sans l'aval de l'opérateur ou du fournisseur du contenu.

C.1.2 attaques par refus de service (DoS, *denial of service*): les attaques par refus de service peuvent survenir lorsqu'une entité tierce (attaquant, consommateur mécontent, etc.) interrompt les communications normales et la fourniture de services entre les opérateurs et leurs abonnés. Des transmissions de données fautives, venant de ce qui semble être un dispositif ou une source valide, peuvent être injectées dans le réseau du domicile et dégrader sévèrement les fonctions normales. Ces transmissions de données fautives peuvent s'étendre au réseau de câble HFC de l'opérateur et y causer des problèmes de performances.

C.1.3 confidentialité du service: la menace visant la confidentialité du service implique une tierce partie (voisins, attaquant, etc.) surveillant/recevant des informations sur un abonné et sur les services qu'il utilise. Cela peut provoquer le vol de mots de passe ou d'informations sur la configuration des dispositifs, ce qui permet aux attaquants d'obtenir ultérieurement accès aux ressources du réseau et à des fichiers/données confidentiels de l'abonné.

C.2 Mesures préventives

Un certain nombre de méthodes différentes peuvent être utilisées pour prévenir les dangers mentionnés ci-dessus concernant le réseau du domicile. Malheureusement, une seule méthode ne peut tous les prévenir, mais une combinaison de plusieurs méthodes peut être la meilleure ligne de défense. On peut utiliser les mesures préventives suivantes:

C.2.1 authentification: l'authentification implique la vérification du fait que les entités expéditrice et réceptrice sont bien ce qu'elles prétendent être. Cela inclut la source du service, le dispositif récepteur et l'abonné.

L'authentification aide à prévenir le vol de service en validant les dispositifs et les utilisateurs d'extrémité, mais n'empêche pas la copie illégale des contenus ni ne prévient l'accès non autorisé de tierces parties qui surveilleraient la liaison. Elle est efficace dans la prévention des attaques par refus de service parce que le trafic peut être rejeté s'il ne vient pas d'une source valide. Par elle-même, l'authentification ne fournit aucun support de confidentialité de service et il faut utiliser le chiffrement.

C.2.2 protection contre la copie: les méthodes de protection contre la copie limitent la capacité d'un dispositif récepteur à faire des copies non autorisées du contenu du service.

La protection contre la copie aide à prévenir le vol de service en limitant le nombre de copies qui peuvent être faites, mais ne protège pas contre l'accès non autorisé aux services. Elle ne protège pas non plus contre le refus de service et n'assure pas la protection de la confidentialité du service. En général, cette mesure préventive est implémentée à des couches d'application plus élevées.

C.2.3 chiffrement des données: le chiffrement des données empêche la découverte et l'accès non autorisés aux données.

Le chiffrement des données est efficace pour la confidentialité des données et la protection contre le vol de service. Le chiffrement empêche de lire les données en l'absence de la clé de déchiffrement correcte, cependant, il ne valide pas les entités source ou de réception et il ne donne pas de

protection contre la copie après déchiffrement des données. Il ne protège pas non plus contre les attaques par refus de service.

C.2.4 pare-feu: les applications de pare-feu empêchent le trafic du réseau de passer d'un domaine à l'autre à moins qu'il ne satisfasse à certains critères établis par l'abonné ou l'opérateur. Dans les applications résidentielles, les pare-feu sont typiquement situés dans les dispositifs de passerelle résidentielle qui connectent le réseau de câble HFC au réseau du domicile.

Une application de pare-feu aide à prévenir les attaques par refus de service et les attaques contre la confidentialité à partir du côté régional (WAN) du pare-feu, mais elle n'empêche pas ce type d'attaques venant du côté résidentiel du pare-feu. Elle ne protège pas non plus contre le vol de service.

C.2.5 sécurité des messages de gestion: cette méthode de prévention implique l'authentification et le chiffrement des seuls messages de gestion du réseau. Les messages de gestion du réseau sont utilisés pour la configuration des dispositifs, pour la commande/surveillance du réseau, pour l'approvisionnement en service, et pour les réservations de qualité de service (QS).

La sécurité des messages de gestion est un bon mécanisme de prévention des attaques par refus de service grâce à l'authentification et au chiffrement des messages de gestion. Les informations de configuration du réseau et les informations personnelles de l'abonné sont aussi protégées contre les attaques contre la confidentialité, mais le contenu du service ne l'est pas. Aussi la sécurité des messages de gestion n'empêche pas le vol du contenu du service par des entités non autorisées.

Annexe D

Applications de traduction CAT et de pare-feu

L'existence des fonctions de traduction NAT et de pare-feu est connue pour interrompre un certain nombre de protocoles et d'applications. Les protocoles et applications dont la liste figure ci-après DOIVENT fonctionner dans toutes les implémentations de traduction CAT et de pare-feu IPCable2Home. Cette liste ne donne PAS d'ordre de priorité.

1) protocole FTP;
2) application d'homologue à homologue (comme Gnutella, LimeWire, BearShare, Morpheus, etc.);
3) IPSec;
4) multidiffusion IGMP et IP;
5) H.323 (utilisé dans Windows pour diverses applications);
6) applications de messagerie instantanée (comme AOL, Microsoft, Yahoo, etc.);
7) courrier électronique (protocoles SMTP et POP);
8) applications de média en temps réel (c'est-à-dire, Real, MediaPlayer, etc.).

De plus, les vendeurs DEVRAIENT faire tout leur possible afin de prendre en charge les applications de jeu en ligne par implémentations de traductions CAT et de pare-feu.

Le document RFC 3235 décrit un certain nombre de directives permettant de créer des applications de façon qu'elles ne soient pas compromises lors d'une exploitation en présence de la fonctionnalité de conversion d'adresse de réseau. Il est fortement recommandé que les développeurs d'applications destinées à fonctionner dans un environnement IPCable2Home suivent ces directives.

Annexe E

Bases MIB

E.1 Base MIB de service portail (PS)

La base MIB de dispositif PSDev DOIT être implémentée comme défini ci-dessous.

```
CABH-PS-DEV-MIB DEFINITIONS ::= BEGIN
IMPORTS
   MODULE-IDENTITY,
   OBJECT-TYPE,
   Integer32,
   NOTIFICATION-TYPE                  FROM SNMPv2-SMI
   TruthValue,


   PhysAddress,
   DateAndTime,
   TEXTUAL-CONVENTION                 FROM SNMPv2-TC
   SnmpAdminString                    FROM SNMP-FRAMEWORK-MIB
   OBJECT-GROUP,
   MODULE-COMPLIANCE,
   NOTIFICATION-GROUP                 FROM SNMPv2-CONF

   InetAddressType,
   InetAddress,
   InetAddressIPv4,
   InetAddressIPv6                    FROM INET-ADDRESS-MIB

   docsDevSwCurrentVers,
   docsDevEvLevel,
   docsDevEvId,
   docsDevEvText,
   docsDevSwFilename,
   docsDevSwServer                    FROM DOCS-CABLE-DEVICE-MIB -- RFC 2669

   cabhCdpServerDhcpAddress,
   cabhCdpWanDataAddrClientId,
   cabhCdpLanTransThreshold           FROM CABH-CDP-MIB

   clabProjCableHome                  FROM CLAB-DEF-MIB;

--============================================================================
--
--   Historique:
--
--
--============================================================================


abhPsDevMib MODULE-IDENTITY
    LAST-UPDATED    "0209200000Z"-- 20 septembre, 2002
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
                    400 Centennial Parkway
                    Louisville, Colorado 80027-1266
                    U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
```

```
    DESCRIPTION
            "Le présent module de base MIB fournit les objets de gestion de base
             pour le dispositif PS. Ce paramètre du dispositif PS décrit
             les attributs généraux du dispositif PS et ses caractéristiques
             comportementales.
             L'essentiel de la base MIB du dispositif PS est nécessaire pour le
             téléchargement d'importation du fichier de configuration."


    ::=  { clabProjCableHome 1 }

-- Conventions textuelles
     X509Certificate ::= TEXTUAL-CONVENTION
       STATUS current
       DESCRIPTION
               "Certificat numérique X.509 codé sous forme d'objet ASN.1 en
règles DER."
       SYNTAX OCTET STRING (SIZE (0..4096))


cabhPsDevMibObjects    OBJECT IDENTIFIER ::= { cabhPsDevMib 1 }
cabhPsDevBase        OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 1 }
cabhPsDevProv     OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 2 }

--
-- le groupe suivant décrit les objets de base contenus dans le dispositif PS.
-- Ce sont des paramètres qui dépendent du dispositif.
--

cabhPsDevDateTime OBJECT-TYPE
        SYNTAX      DateAndTime
        MAX-ACCESS  read-write
        STATUS      current
        DESCRIPTION
            "La date et l'heure, avec des informations facultatives sur le
fuseau horaire."
    ::= { cabhPsDevBase 1 }

cabhPsDevResetNow       OBJECT-TYPE
SYNTAX                  TruthValue
MAX-ACCESS    read-write
STATUS                  current
DESCRIPTION
"Le fait de mettre cet objet à la valeur true(1) provoque le redémarrage du
dispositif PS autonome ou imbriqué. Le code du dispositif s'initialise comme si
le dispositif démarrait à partir d'une remise sous tension. Le portail CMP fait
en sorte que les valeurs d'objet de base persistent comme spécifié. La lecture
de cet objet renvoie toujours la valeur false(2)."
::= { cabhPsDevBase 2 }

cabhPsDevSerialNumber OBJECT-TYPE
SYNTAX      SnmpAdminString (SIZE (0..128))
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
    "Numéro de série du constructeur pour ce dispositif PS. Ce paramètre
    est fourni par le constructeur et est conservé en mémoire non volatile."
::= { cabhPsDevBase 3 }

cabhPsDevHardwareVersion OBJECT-TYPE
SYNTAX      SnmpAdminString (SIZE (0..48))
MAX-ACCESS  read-only
STATUS      current
```

```
DESCRIPTION
    "Version matérielle du constructeur pour ce dispositif PS. Ce paramètre est
     fourni par le constructeur et est conservé en mémoire non volatile."
::= { cabhPsDevBase 4 }

cabhPsDevWanManMacAddress OBJECT-TYPE
SYNTAX      PhysAddress
MAX-ACCESS  read-only
STATUS      current
DESCRIPTION
"Adresse MAC à l'interface PS/WAN-MAN. C'est l'adresse matérielle du dispositif
PS à utiliser par le client CDC afin d'identifier de façon unique le service PS
auprès du serveur DHCP du réseau de transmission de données par câble pour
l'acquisition d'une adresse IP à utiliser pour la messagerie de gestion entre le
système NMS du réseau câblé et le portail CMP."


::= { cabhPsDevBase 5 }

cabhPsDevWanDataMacAddress OBJECT-TYPE
     SYNTAX      PhysAddress
     MAX-ACCESS  read-only
     STATUS      current
     DESCRIPTION
       "Adresse MAC à l'interface PS/WAN-Data. Le service PS peut avoir de
       multiples interfaces avec le réseau WAN-Data, qui partageront la même
       adresse matérielle. Les identificateurs de client seront uniques de façon
       que chacun puisse se faire assigner une adresse IP différente et unique."

    ::= { cabhPsDevBase 6 }

cabhPsDevTypeIdentifier    OBJECT-TYPE
     SYNTAX      SnmpAdminString
     MAX-ACCESS  read-only
     STATUS      current
     DESCRIPTION
       "C'est une copie de l'identificateur de type de dispositif utilisé
       dans l'option DHCP 60 échangée entre le service PS et le serveur DHCP."
     ::= { cabhPsDevBase 7 }

cabhPsDevSetToFactory    OBJECT-TYPE
     SYNTAX      TruthValue
     MAX-ACCESS  read-write
     STATUS      current
     DESCRIPTION
       "Le fait de mettre cet objet à la valeur true(1) règle tous les objets de
       base MIB de dispositif PsDev aux valeurs par défaut de l'usine. La
       lecture de cet objet renvoie toujours la valeur false(2)."

    ::= { cabhPsDevBase 8 }

cabhPsDevWanManClientId    OBJECT-TYPE
     SYNTAX      OCTET STRING (SIZE (1..80))
     MAX-ACCESS  read-write
     STATUS      current
     DESCRIPTION
       "C'est l'identificateur de client utilisé pour les demandes DHCP de
       réseau WAN-Man. La valeur par défaut est l'adresse MAC de 6 octets."
::= { cabhPsDevBase 9 }

cabhPsDevTodSyncStatus OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
       "Cet objet indique si le service PS a été capable de se synchroniser
       correctement avec le serveur d'heure actuelle (ToD) situé dans le réseau
       câblé. Le service PS règle cet objet à la valeur true(1) si le service PS
       réussit à synchroniser son heure avec le serveur ToD. Le service PS règle
       cet objet à la valeur false(2) si le service PS ne réussit pas à se
       synchroniser avec le serveur ToD."
    DEFVAL { false }
::= { cabhPsDevBase 10 }

cabhPsDevProvMode  OBJECT-TYPE
     SYNTAX    INTEGER
     {
       dhcpmode(1),
       snmpmode(2)
     }
     MAX-ACCESS  read-only
     STATUS    current
     DESCRIPTION
       "Cet objet indique le mode d'approvisionnement dans lequel le dispositif
       PS fonctionne actuellement. Si le service PS fonctionne actuellement dans
       le mode d'approvisionnement DHCP, le service PS met cet objet à la valeur
       dhcpmode(1). Si le service PS fonctionne actuellement dans le mode
       d'approvisionnement SNMP, le service PS règle cet objet à la valeur
       snmpmode(2)."
::={ cabhPsDevBase 11 }



--
--   Le groupe suivant définit les paramètres spécifiques d'approvisionnement
--

cabhPsDevProvisioningTimer OBJECT-TYPE
     SYNTAX      INTEGER (0..16383)
     UNITS    "minutes"
     MAX-ACCESS  read-write
     STATUS      current
     DESCRIPTION
       "Cet objet permet à l'utilisateur de régler la durée du temporisateur
       d'approvisionnement. La valeur est exprimée en minutes. Le réglage du
       temporisateur à 0 le désactive. La valeur par défaut du temporisateur
       est 5."
     DEFVAL {5}
     ::=  {cabhPsDevProv 1}

cabhPsDevProvConfigFile OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..128))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "URL du serveur TFTP pour le téléchargement d'importation des paramètres
       d'approvisionnement et de configuration vers ce dispositif. Renvoie la
       valeur NULL si l'adresse du serveur est inconnue."
    ::= { cabhPsDevProv 2 }

cabhPsDevProvConfigHash OBJECT-TYPE
     SYNTAX OCTET STRING (SIZE(20))
     MAX-ACCESS read-write
     STATUS current
```

```
     DESCRIPTION
        "Hachage du contenu du fichier de configuration, calculé et
        envoyé au service PS avant l'envoi du fichier de configuration.
        Pour l'algorithme d'authentification SHA-1, la longueur du hachage
        est de 160 bits."
     ::= { cabhPsDevProv 3 }

cabhPsDevProvConfigFileSize OBJECT-TYPE
     SYNTAX    Integer32
     UNITS    "bytes"
     MAX-ACCESS  read-only
     STATUS    current
     DESCRIPTION
          "Taille du fichier de configuration."
     ::={ cabhPsDevProv 4 }

cabhPsDevProvConfigFileStatus OBJECT-TYPE
     SYNTAX    INTEGER
     {
            idle      (1),
            busy    (2)
     }
     MAX-ACCESS  read-only
     STATUS    current
     DESCRIPTION
       "Cet objet indique l'état actuel du processus de téléchargement du
       fichier de configuration. Il sert à indiquer à l'entité de gestion que
       le service PS rejettera les déclencheurs du fichier de configuration PS
       (demande Set selon l'objet cabhPsDevProvConfigFile) lorsqu'il sera
       occupé."
     ::={ cabhPsDevProv 5 }

cabhPsDevProvConfigTLVProcessed OBJECT-TYPE
     SYNTAX    INTEGER (0..16383)
     MAX-ACCESS  read-only
     STATUS    current
     DESCRIPTION
        "Nombre d'éléments TLV traités dans le fichier de configuration."
     ::={ cabhPsDevProv 6 }

cabhPsDevProvConfigTLVRejected OBJECT-TYPE
     SYNTAX    INTEGER (0..16383)
     MAX-ACCESS  read-only
     STATUS    current
     DESCRIPTION
        "Nombre d'éléments TLV rejetés dans le fichier de configuration."
     ::={ cabhPsDevProv 7 }

cabhPsDevProvSolicitedKeyTimeout OBJECT-TYPE
   SYNTAX      Integer32 (15..600)
   UNITS  "seconds"
   MAX-ACCESS  read-write
   STATUS      current
     DESCRIPTION
        "Cette temporisation n'est applicable que lorsque le serveur
        d'approvisionnement a lancé la gestion de clé (par un message de réveil)
        en version SNMPv3. C'est la période pendant laquelle le service PS
        sauvegarde un nombre (dans le champ de numéro de séquence) extrait de
        la demande AP envoyée et attend la réponse AP correspondante en
        provenance du serveur d'approvisionnement."
     DEFVAL { 120 }
     ::= { cabhPsDevProv 8 }
```

```
cabhPsDevProvState    OBJECT-TYPE
    SYNTAX      INTEGER
    {
            pass        (1),
            inProgress  (2),
            fail        (3)
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Cet objet indique l'état d'avancement du processus d'initialisation.
       Les états de succès ou d'échec apparaissent après achèvement du flux
       d'initialisation. L'état 'InProgress' apparaît du début à la fin de
       l'initialisation du dispositif PS."
    ::= { cabhPsDevProv 9 }

cabhPsDevProvAuthState    OBJECT-TYPE
    SYNTAX      INTEGER
    {
            accepted    (1),
            rejected    (2)
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Cet objet indique l'état d'authentification du fichier de
       configuration."
    ::= { cabhPsDevProv 10 }

cabhPsDevProvCorrelationId OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Valeur aléatoire générée par le service PS pour utilisation dans
       l'autorisation d'enregistrement. Elle est destinée à n'être utilisée
       que dans les messages d'initialisation du service PS et pour le
       téléchargement de fichier de configuration PSdownload. Cette valeur
       apparaît dans les deux objets cabhPsDevProvisioningStatus et
       cabhPsDevProvisioningEnrollmentReport contenus dans des messages INFORM
       destinés à vérifier l'instance de chargement du fichier de
       configuration."

    ::= { cabhPsDevProv 11 }

cabhPsDevTimeServerAddrType OBJECT-TYPE
        SYNTAX      InetAddressType
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
           "Le type d'adresse IP du serveur temporel(RFC-868). La version IP 4
           est normalement utilisée."
    ::= { cabhPsDevProv 12 }

cabhPsDevTimeServerAddr OBJECT-TYPE
        SYNTAX      InetAddress
        MAX-ACCESS  read-only
        STATUS      current
        DESCRIPTION
           "L'adresse IP du serveur temporel(RFC-868). Renvoie
           0.0.0.0 si l'adresse IP du serveur temporel est inconnue."
    ::= { cabhPsDevProv 13 }
```

```
--
-- Ce groupe de notifications fera l'objet d'extensions futures.
--

cabhPsNotification OBJECT IDENTIFIER ::= { cabhPsDevMib 2 0 }
cabhPsConformance  OBJECT IDENTIFIER ::= { cabhPsDevMib 3 }
cabhPsCompliances  OBJECT IDENTIFIER ::= { cabhPsConformance 1 }
cabhPsGroups       OBJECT IDENTIFIER ::= { cabhPsConformance 2 }

--
--    Groupe de notifications
--

cabhPsDevInitTLVUnknownTrap     NOTIFICATION-TYPE
   OBJECTS   {
      docsDevEvLevel,
      docsDevEvId,
      docsDevEvText,
      cabhPsDevWanManMacAddress
   }
   STATUS  current
   DESCRIPTION
      "Événement dû à la détection d'éléments TLV inconnus pendant le processus
      d'analyse des éléments TLV. Les valeurs des objets docsDevEvLevel,
      docsDevEvId, et docsDevEvText sont extraites de l'entrée qui journalise
      cet événement dans la table docsDevEventTable. La valeur de l'objet
      cabhPsDevWanManMacAddress indique l'adresse MAC du réseau Wan-Man du PS.
      Cette partie des informations est uniforme dans tous les messages TRAP du
      service PS."
   ::= { cabhPsNotification 1 }

cabhPsDevInitTrap  NOTIFICATION-TYPE
   OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
      cabhPsDevWanManMacAddress,
        cabhPsDevProvConfigFile,
        cabhPsDevProvConfigTLVProcessed,
        cabhPsDevProvConfigTLVRejected
   }
   STATUS      current
   DESCRIPTION
      "Ce message Inform est envoyé afin de confirmer l'achèvement correct
      du processus d'approvisionnement."
   ::= { cabhPsNotification 2 }

cabhPsDevInitRetryTrap  NOTIFICATION-TYPE
   OBJECTS  {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
      cabhPsDevWanManMacAddress
   }
   STATUS      current
   DESCRIPTION
      "Evénement destiné à signaler qu'une panne s'est produite pendant le
      processus d'initialisation et a été détectée dans le service PS."
   ::= { cabhPsNotification 3 }
```

```
cabhPsDevDHCPFailTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress,
       cabhCdpServerDhcpAddress
   }
   STATUS  current
   DESCRIPTION
      "Evénement destiné à signaler la panne d'un serveur DHCP.
      La valeur de l'objet cabhCdpServerDhcpAddress est l'adresse IP
      du serveur DHCP."
   ::= { cabhPsNotification 4 }


cabhPsDevSwUpgradeInitTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress,
       docsDevSwFilename,
       docsDevSwServer
   }
   STATUS  current
   DESCRIPTION
      "Evénement destiné à signaler un événement de lancement de mise à jour
      logicielle. Les valeurs des objets docsDevSwFilename et docsDevSwServer
      indiquent le nom de l'image logicielle et l'adresse IP du serveur dont
      l'image provient."
   ::= { cabhPsNotification 5 }


cabhPsDevSwUpgradeFailTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress,
       docsDevSwFilename,
       docsDevSwServer
   }
   STATUS  current
   DESCRIPTION
      "Evénement destiné à signaler la panne d'un essai de mise à jour
      logicielle. Les valeurs des objets docsDevSwFilename et
      docsDevSwServer indiquent le nom de l'image logicielle
      et l'adresse IP du serveur dont l'image provient."
   ::= { cabhPsNotification 6 }


cabhPsDevSwUpgradeSuccessTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress,
       docsDevSwFilename,
       docsDevSwServer
   }
```

```
   STATUS  current
   DESCRIPTION
      "Evénement destiné à signaler l'événement de succès de la mise
      à jour logicielle. Les valeurs des objets docsDevSwFilename et
      docsDevSwServer indiquent le nom de l'image logicielle
      et l'adresse IP du serveur dont l'image provient."
   ::= { cabhPsNotification 7 }


cabhPsDevSwUpgradeCVCFailTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress
   }
   STATUS  current
   DESCRIPTION
       "Evénement destiné à signaler qu'un échec de vérification
       du fichier de code s'est produit pendant une tentative de mise à jour
       logicielle sécurisée."

   ::= { cabhPsNotification 8 }


cabhPsDevTODFailTrap NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevTimeServerAddr,
       cabhPsDevWanManMacAddress
   }
   STATUS  current
   DESCRIPTION
      "Evénement destiné à signaler la panne d'un serveur ToD.
      La valeur de l'objet cabhPsDevTimeServerAddr indique l'adresse IP du
      serveur."

   ::= { cabhPsNotification 9 }

cabhPsDevCdpWanDataIpTrap  NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhCdpWanDataAddrClientId,
       cabhPsDevWanManMacAddress
   }
   STATUS      current
   DESCRIPTION
      "Evénement destiné à signaler l'échec du PS lorsqu'il a cherché
      à obtenir toutes les adresses IP de réseau WAN-Data requises.
      L'objet cabhCdpWanDataAddrClientId indique l'identificateur de
      client pour lequel l'échec s'est produit."

   ::= { cabhPsNotification 10 }


cabhPsDevCdpThresholdTrap  NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
```

```
        cabhPsDevWanManMacAddress,
        cabhCdpLanTransThreshold
    }
    STATUS      current
    DESCRIPTION
       "Evénement destiné à signaler que le seuil du secteur Lan-Trans
       a été dépassé."
    ::= { cabhPsNotification 11 }

cabhPsDevCspTrap  NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
       "Afin de signaler un événement concernant le portail de sécurité par
       câble."
    ::= { cabhPsNotification 12 }

cabhPsDevCapTrap  NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
        "Afin de signaler un événement concernant le portail CAP."
    ::= { cabhPsNotification 13 }

cabhPsDevCtpTrap  NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
       "Afin de signaler un événement concernant le portail CTP."
    ::= { cabhPsNotification 14 }

cabhPsDevProvEnrollTrap  NOTIFICATION-TYPE
    OBJECTS {
        cabhPsDevHardwareVersion,
        docsDevSwCurrentVers,
        cabhPsDevTypeIdentifier,
        cabhPsDevWanManMacAddress,
        cabhPsDevProvCorrelationId
    }
    STATUS      current
    DESCRIPTION
        "Ce message Inform est envoyé afin de lancer le processus
        d'approvisionnement CableHome."
    REFERENCE
         "Message Inform tel que défini dans RFC 1902"
    ::= { cabhPsNotification 15 }
```

```
cabhPsDevCdpLanIpPoolTrap NOTIFICATION-TYPE
     OBJECTS {
     docsDevEvLevel, docsDevEvId, docsDevEvText, cabhPsDevWanManMacAddress,
     cabhCdpLanTransCurCount
     }
     STATUS current
     DESCRIPTION
         "Evénement destiné à signaler que la réserve d'adresses IP pour
         clients de LAN, comme défini par les objets cabhCdpLanPoolStart
         et cabhCdpLanPoolEnd, est épuisée."

     ::= { cabhPsNotification 16}

-- déclarations de conformité

cabhPsBasicCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
       "La déclaration de conformité des dispositifs qui implémentent une
       capacité de service PS."
    MODULE   -- cabhPsMib




-- groupes inconditionnellement obligatoires

    MANDATORY-GROUPS {
            cabhPsGroup
    }

::= { cabhPsCompliances 1}


cabhPsGroup OBJECT-GROUP
    OBJECTS {
         cabhPsDevDateTime,
         cabhPsDevResetNow,
         cabhPsDevSerialNumber,
         cabhPsDevHardwareVersion,
         cabhPsDevWanManMacAddress,
         cabhPsDevWanDataMacAddress,
         cabhPsDevTypeIdentifier,
         cabhPsDevSetToFactory,
         cabhPsDevWanManClientId,
         cabhPsDevTodSyncStatus,
         cabhPsDevProvMode,

         cabhPsDevProvisioningTimer,
         cabhPsDevProvConfigFile,
         cabhPsDevProvConfigHash,
         cabhPsDevProvConfigFileSize,
         cabhPsDevProvConfigFileStatus,
         cabhPsDevProvConfigTLVProcessed,
         cabhPsDevProvConfigTLVRejected,
         cabhPsDevProvSolicitedKeyTimeout,
         cabhPsDevProvState,
         cabhPsDevProvAuthState,
         cabhPsDevProvCorrelationId,
         cabhPsDevTimeServerAddrType,
         cabhPsDevTimeServerAddr

    }
```

```
    STATUS    current
    DESCRIPTION
        "Groupe d'objets pour base MIB de service PS."
    ::= { cabhPsGroups 1 }

cabhPsNotificationGroup     NOTIFICATION-GROUP
     NOTIFICATIONS { cabhPsDevInitTLVUnknownTrap, cabhPsDevInitTrap,
cabhPsDevInitRetryTrap,
                     cabhPsDevDHCPFailTrap, cabhPsDevSwUpgradeInitTrap,
cabhPsDevSwUpgradeFailTrap,
                     cabhPsDevSwUpgradeSuccessTrap, cabhPsDevSwUpgradeCVCFailTrap,
cabhPsDevTODFailTrap,
                     cabhPsDevCdpWanDataIpTrap, cabhPsDevCdpThresholdTrap,
cabhPsDevCspTrap,
                     cabhPsDevCapTrap, cabhPsDevCtpTrap, cabhPsDevProvEnrollTrap }
     STATUS   current
     DESCRIPTION
          "Ces notifications traitent des changements d'état d'un dispositif
          PS."
     ::= { cabhPsGroups 2 }

END
```

E.2 Base MIB de portail d'essai du câble

La base MIB de portail CTP DOIT être implémentée comme défini ci-dessous.

```
CABH-CTP-MIB DEFINITIONS ::= BEGIN
IMPORTS
   MODULE-IDENTITY,
   OBJECT-TYPE
                     FROM SNMPv2-SMI
   TruthValue,
   TEXTUAL-CONVENTION
                     FROM SNMPv2-TC
   OBJECT-GROUP,
   MODULE-COMPLIANCE
                           FROM SNMPv2-CONF
   InetAddressType,
   InetAddress,
   InetAddressIPv4,
   InetAddressIPv6
                                    FROM INET-ADDRESS-MIB
   clabProjCableHome
                     FROM CLAB-DEF-MIB;

--============================================================================
--
--   Historique:
--
--   Date      Modifié par        Raison
--
--============================================================================

cabhCtpMib MODULE-IDENTITY
    LAST-UPDATED  "0209200000Z" -- 20 septembre, 2002
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Adresse postale: Cable Television Laboratories, Inc.
                             400 Centennial Parkway
                             Louisville, Colorado 80027-1266
                             ETATS-UNIS D'AMÉRIQUE
```

```
            Tél:    +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
            "Le présent module de base MIB définit les commandes de diagnostic
            offertes par le portail d'essai du câble (CTP)."

    ::=  { clabProjCableHome 5 }

-- Conventions textuelles


cabhCtpObjects          OBJECT IDENTIFIER ::= { cabhCtpMib 1 }
cabhCtpBase             OBJECT IDENTIFIER ::= { cabhCtpObjects 1 }
cabhCtpConnSpeed                OBJECT IDENTIFIER ::= { cabhCtpObjects 2 }
cabhCtpPing                     OBJECT IDENTIFIER ::= { cabhCtpObjects 3 }

--
--   Le groupe suivant décrit les objets de base contenus dans le portail de
--   gestion par câble.
--

cabhCtpSetToFactory     OBJECT-TYPE
SYNTAX                  TruthValue
MAX-ACCESS   read-write
STATUS                  current
DESCRIPTION
    "Le fait de mettre cet objet à la valeur true(1) provoque l'effacement de
    toutes les tables contenues dans la base MIB de portail CTP et le retour à
    leurs valeurs par défaut de tous les objets de base MIB de portail CTP
    possédant de telles valeurs. La lecture de cet objet renvoie toujours
    la valeur false(2)."
::={cabhCtpBase 1}

--
--   Paramètres et résultats de la commande de vitesse de connexion
--

cabhCtpConnSrcIpType    OBJECT-TYPE
     SYNTAX    InetAddressType
     MAX-ACCESS  read-write
   STATUS      current
   DESCRIPTION
      "Type d'adresse IP utilisée comme adresse d'origine pour l'essai
      de vitesse de connexion."
     DEFVAL { ipv4 }
::= { cabhCtpConnSpeed 1 }

cabhCtpConnSrcIp OBJECT-TYPE
     SYNTAX    InetAddress
     MAX-ACCESS  read-write
   STATUS      current
   DESCRIPTION
      "Adresse IP utilisée comme adresse d'origine pour l'essai de vitesse
      de connexion. La valeur par défaut est celle de l'objet
      cabhCdpServerRouter (192.168.0.1)."
     REFERENCE
          "Section 6.4.4 de la spécification"
     DEFVAL { 'c0a80001'h }  -- 192.168.0.1
     ::= { cabhCtpConnSpeed 2 }

cabhCtpConnDestIpType   OBJECT-TYPE
     SYNTAX    InetAddressType
     MAX-ACCESS  read-write
```

```
STATUS    current
DESCRIPTION
    "Type d'adresse IP utilisée comme adresse de destination de l'utilitaire
    de vitesse de connexion du portail CTP."
     DEFVAL { ipv4 }
::={ cabhCtpConnSpeed 3 }



cabhCtpConnDestIp  OBJECT-TYPE
     SYNTAX         InetAddress
     MAX-ACCESS     read-write
    STATUS          current
    DESCRIPTION
       "Type d'adresse IP utilisée comme adresse de destination pour l'essai
       de vitesse de connexion."
     ::= { cabhCtpConnSpeed 4 }

cabhCtpConnProto OBJECT-TYPE
     SYNTAX    INTEGER {
              udp        (1),
              tcp        (2)
              }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Protocole utilisé dans l'essai de vitesse de connexion. L'essai du
       portail TCP est facultatif."
    DEFVAL { udp }
     ::= { cabhCtpConnSpeed 5 }


cabhCtpConnNumPkts OBJECT-TYPE
    SYNTAX    INTEGER (1..65535)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Nombre de paquets que le portail CTP doit envoyer lorsqu'il reçoit
       l'ordre d'exécuter l'utilitaire de vitesse de connexion."
     DEFVAL { 100 }
     ::= { cabhCtpConnSpeed 6 }

cabhCtpConnPktSize OBJECT-TYPE
     SYNTAX    INTEGER (64..1518)
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Taille des trames d'essai."
     REFERENCE
       ""
     DEFVAL { 1518 }
     ::= { cabhCtpConnSpeed 7 }

cabhCtpConnTimeOut OBJECT-TYPE
     SYNTAX    INTEGER (0..600000)            -- Max 10 minutes
     UNITS    "milliseconds"
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Valeur de temporisation pour la réponse. Une valeur de zéro
       indique l'absence de temporisation et ne peut être utilisée que
       pour le portail TCP."
     DEFVAL {30000}  -- 30 secondes
    ::= { cabhCtpConnSpeed 8 }
```

```
cabhCtpConnControl OBJECT-TYPE
SYNTAX    INTEGER {
     start(1),
     abort(2)
     }
MAX-ACCESS    read-write
STATUS    current
DESCRIPTION
    "Commande pour l'utilitaire de vitesse de connexion. Le fait de mettre
    cet objet à la valeur start(1) provoque l'exécution de l'utilitaire de
    vitesse de connexion. Le fait de mettre cet objet à la valeur abort(2)
    provoque l'arrêt de l'exécution de l'utilitaire de vitesse de connexion.
    Ce paramètre ne devrait être réglé qu'en protocole SNMP."
DEFVAL  {abort }
::={ cabhCtpConnSpeed 9 }



cabhCtpConnStatus  OBJECT-TYPE
SYNTAX    INTEGER {
     notRun(1),
     running(2),
complete(3),
aborted(4),
timedOut(5)
     }
MAX-ACCESS    read-only
STATUS    current
DESCRIPTION
   "État de l'utilitaire de vitesse de connexion."
DEFVAL   { notRun }
::={ cabhCtpConnSpeed 10 }


cabhCtpConnPktsSent     OBJECT-TYPE
     SYNTAX    INTEGER (0..65535)
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Nombre de paquets que le portail CTP a envoyés après avoir reçu
        l'ordre d'exécuter l'utilitaire de vitesse de connexion."
     ::= { cabhCtpConnSpeed 11 }

cabhCtpConnPktsRecv     OBJECT-TYPE
     SYNTAX    INTEGER (0..65535)
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Nombre de paquets que le portail CTP a reçus après avoir exécuté
       l'utilitaire de vitesse de connexion."
     ::= { cabhCtpConnSpeed 12 }

cabhCtpConnRTTOBJECT-TYPE
     SYNTAX   INTEGER (0..600000)
     UNITS    "millisec"
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Temps d'aller-retour résultant pour l'ensemble des paquets envoyés à
       destination -et reçus en provenance- du dispositif IP de réseau LAN
       cible."
     ::= { cabhCtpConnSpeed 13 }
```

```
cabhCtpConnThroughput   OBJECT-TYPE
     SYNTAX    INTEGER (0..65535)
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Débit utile moyen d'aller-retour mesuré en kilobits par seconde."
     ::= { cabhCtpConnSpeed 14 }



--
--   Paramètres et résultats pour la commande de validation par écho
--

cabhCtpPingSrcIpType    OBJECT-TYPE
SYNTAX    InetAddressType
MAX-ACCESS    read-write
STATUS    current
DESCRIPTION
    "Type d'adresse IP d'origine de l'utilitaire de validation par écho du
    portail CTP."
DEFVAL { ipv4 }
::={ cabhCtpPing 1 }

cabhCtpPingSrcIp OBJECT-TYPE
     SYNTAX    InetAddress
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Adresse IP utilisée comme adresse d'origine pour l'essai de validation
       par écho. La valeur par défaut est celle de l'objet CabhCdpServerRouter
      (192.168.0.1)."
    REFERENCE
             "Section 6.4.4 de la spécification"
    DEFVAL { 'c0a80001'h }
     ::= { cabhCtpPing 2 }

cabhCtpPingDestIpType   OBJECT-TYPE
SYNTAX    InetAddressType
MAX-ACCESS    read-write
STATUS    current
DESCRIPTION
    "Type d'adresse IP de destination de l'utilitaire de validation par écho
    du portail CTP."
DEFVAL { ipv4 }
::={ cabhCtpPing 3 }

cabhCtpPingDestIp  OBJECT-TYPE
     SYNTAX    InetAddress
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Adresse IP de destination utilisée pour l'essai de validation par écho."
     ::= { cabhCtpPing 4 }

cabhCtpPingNumPkts OBJECT-TYPE
     SYNTAX    INTEGER (1..4)
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Nombre de paquets à envoyer à chaque serveur."
     DEFVAL {1}
     ::= { cabhCtpPing 5 }
```

```
cabhCtpPingPktSize OBJECT-TYPE
     SYNTAX    INTEGER (64..1518)
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Taille des trames d'essai."
     DEFVAL {64}
     ::= { cabhCtpPing 6 }

cabhCtpPingTimeBetween  OBJECT-TYPE
     SYNTAX    INTEGER (0..600000)
     UNITS    "millisecondes"
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Durée écoulée entre l'envoi d'une validation par écho et la suivante."
     DEFVAL { 1000 }
    ::= { cabhCtpPing 7 }

cabhCtpPingTimeOut      OBJECT-TYPE
SYNTAX    INTEGER (1..600000)
UNITS     "milliseconds"
MAX-ACCESS   read-write
STATUS    current
DESCRIPTION
    "Temporisation de la réponse de validation par écho (réponse ICMP) pour
    une unique transmission de message de validation par écho (demande ICMP)."
DEFVAL  { 5000 } -- 5 secondes
::={ cabhCtpPing 8 }



cabhCtpPingControl OBJECT-TYPE
SYNTAX    INTEGER {
     start(1),
     abort(2)
     }
MAX-ACCESS   read-write
STATUS    current
DESCRIPTION
    "Commande de l'utilitaire de validation par écho. Le fait de mettre cet
    objet à la valeur start(1) provoque l'exécution de l'utilitaire de
    validation par écho. Le fait de mettre cet objet à la valeur abort(2)
    provoque l'arrêt de l'exécution de l'utilitaire de validation par écho.
    Ce paramètre ne devrait être réglé qu'en protocole SNMP."
DEFVAL  {abort }
::={ cabhCtpPing 9 }


cabhCtpPingStatus  OBJECT-TYPE
SYNTAX    INTEGER {
     notRun(1),
     running(2),
complete(3),
aborted(4),
timedOut(5)
     }
MAX-ACCESS   read-only
STATUS    current
DESCRIPTION
   "Etat de l'utilitaire de validation par écho."
DEFVAL   { notRun }
::={ cabhCtpPing 10 }
```

```
cabhCtpPingNumSent      OBJECT-TYPE
SYNTAX    INTEGER (0..4)
MAX-ACCESS   read-only
STATUS    current
DESCRIPTION
    "Nombre de validations envoyées."
::={ cabhCtpPing 11 }

cabhCtpPingNumRecv OBJECT-TYPE
     SYNTAX    INTEGER (0..255)
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Nombre de validations reçues."
     ::= { cabhCtpPing 12 }

cabhCtpPingAvgRTT  OBJECT-TYPE
     SYNTAX    INTEGER (0..600000)
     UNITS     "millisec"
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Moyenne résultante des temps d'aller-retour des paquets acquittés."
     ::= { cabhCtpPing 13 }

cabhCtpPingMaxRTT  OBJECT-TYPE
     SYNTAX    INTEGER (0..600000)
     UNITS     "millisec"
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Temps d'aller-retour maximal résultant des paquets acquittés."
     ::= { cabhCtpPing 14 }

cabhCtpPingMinRTT  OBJECT-TYPE
     SYNTAX    INTEGER (0..600000)
     UNITS     "millisec"
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Temps d'aller-retour minimal résultant des paquets acquittés."
     ::= { cabhCtpPing 15 }

cabhCtpPingNumIcmpError OBJECT-TYPE
     SYNTAX    INTEGER (0..255)
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Nombre d'erreurs ICMP."
     ::= { cabhCtpPing 16 }

cabhCtpPingIcmpError    OBJECT-TYPE
     SYNTAX    INTEGER (0..255)
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Dernière erreur ICMP."
     ::= { cabhCtpPing 17 }
```

```
--============================================================================

--
-- Ce groupe de notifications fera l'objet d'extensions futures.
--

cabhCtpNotification OBJECT IDENTIFIER ::= { cabhCtpMib 2 0 }
cabhCtpConformance  OBJECT IDENTIFIER ::= { cabhCtpMib 3 }
cabhCtpCompliances  OBJECT IDENTIFIER ::= { cabhCtpConformance 1 }
cabhCtpGroups       OBJECT IDENTIFIER ::= { cabhCtpConformance 2 }

--
--    Groupe de notifications
--

-- déclarations de conformité

cabhCtpBasicCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
       "La déclaration de conformité des dispositifs qui implémentent la
       capacité de service portail."
    MODULE   --cabhCtpMib



-- groupes inconditionnellement obligatoires

    MANDATORY-GROUPS {
            cabhCtpGroup
    }

::= { cabhCtpCompliances 3 }


cabhCtpGroup OBJECT-GROUP
    OBJECTS {

        cabhCtpSetToFactory,
        cabhCtpConnSrcIpType,
        cabhCtpConnSrcIp,
        cabhCtpConnDestIpType,
        cabhCtpConnDestIp,
        cabhCtpConnProto,
        cabhCtpConnNumPkts,
        cabhCtpConnPktSize,
        cabhCtpConnTimeOut,
        cabhCtpConnControl,
        cabhCtpConnStatus,
        cabhCtpConnPktsSent,
        cabhCtpConnPktsRecv,
        cabhCtpConnRTT,
        cabhCtpConnThroughput,

        cabhCtpPingSrcIpType,
        cabhCtpPingSrcIp,
        cabhCtpPingDestIpType,
        cabhCtpPingDestIp,
        cabhCtpPingNumPkts,
        cabhCtpPingPktSize,
        cabhCtpPingTimeBetween,
        cabhCtpPingTimeOut,
        cabhCtpPingControl,
```

```
        cabhCtpPingStatus,
        cabhCtpPingNumSent,
        cabhCtpPingNumRecv,
        cabhCtpPingAvgRTT,
        cabhCtpPingMinRTT,
        cabhCtpPingMaxRTT,
        cabhCtpPingNumIcmpError,
        cabhCtpPingIcmpError
     }
    STATUS    current
    DESCRIPTION
        "Groupe d'objets pour base MIB de portail CTP."
    ::= { cabhCtpGroups 1 }

END
```

E.3 Base MIB de sécurité

La base MIB de sécurité (SEC) DOIT être implémentée comme défini ci-dessous.

```
CABH-SEC-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
     Unsigned32,
     BITS,
     OBJECT-TYPE    FROM SNMPv2-SMI
     TruthValue,
     DisplayString,
     TimeStamp   FROM SNMPv2-TC
     OBJECT-GROUP,
     MODULE-COMPLIANCE  FROM SNMPv2-CONF
     InetAddressIPv4         FROM INET-ADDRESS-MIB
     SnmpAdminString         FROM SNMP-FRAMEWORK-MIB -- RFC 2571
     X509Certificate         FROM DOCS-BPI2-MIB
     clabProjCableHome  FROM CLAB-DEF-MIB;

--============================================================================
--
--   Historique:
--
--   Date      Modifié par        Raison
--
--
--============================================================================

cabhSecMib MODULE-IDENTITY
    LAST-UPDATED    "0209200000Z" -- 20 septembre, 2002
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Adresse postale:     Cable Television Laboratories, Inc.
                       400 Centennial Parkway
                       Louisville, Colorado 80027-1266
                       ETATS-UNIS D'AMÉRIQUE
            Tél:    +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
            "Le présent module de base MIB fournit les objets de gestion de base
            pour les services portail de sécurité.
```

```
    ::=  { clabProjCableHome 2 }

-- Conventions textuelles


cabhSecFwObjects   OBJECT IDENTIFIER ::= { cabhSecMib 1 }
cabhSecFwBase          OBJECT IDENTIFIER ::= { cabhSecFwObjects 1 }
cabhSecFwLogCtl    OBJECT IDENTIFIER ::= { cabhSecFwObjects 2 }
cabhSecCertObjects     OBJECT IDENTIFIER ::= { cabhSecMib 2 }
--
--   Le groupe suivant décrit les objets de base contenus dans le pare-feu Cable
--   Home.
--

cabhSecFwPolicyFileEnable OBJECT-TYPE
     SYNTAX      INTEGER {
                 enable          (1),
                 disable    (2)
                 }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Ce paramètre indique s'il convient ou non d'activer la capacité de
        pare-feu."
     DEFVAL {enable}
    ::= { cabhSecFwBase 1 }

cabhSecFwPolicyFileURL OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Cet objet contient le nom et l'adresse IP du fichier contenant
        l'ensemble des règles de politique en format d'URL de protocole TFTP.
        Une fois que cet objet a été mis à jour, il déclenche le téléchargement
        du fichier."

::= { cabhSecFwBase 2 }



cabhSecFwPolicyFileHash OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE(20))
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
        "Hachage du contenu du fichier d'ensemble de règles, calculé et
        envoyé au service PS avant l'envoi du fichier d'ensemble de règles.
        Dans l'algorithme d'authentification SHA-1, la longueur du hachage est
        de 160 bits. Cette valeur de hachage est codée en format binaire."

::= { cabhSecFwBase 3 }


cabhSecFwPolicyFileOperStatus OBJECT-TYPE
     SYNTAX   INTEGER    {
                 inProgress(1),
                 completeFromProvisioning(2),
                 completeFromMgt(3),
                 failed(4)
     }
     MAX-ACCESS read-only
     STATUS current
```

```
     DESCRIPTION
        "La valeur InProgress(1) indique qu'un téléchargement TFTP est en cours,
        soit à cause d'une divergence de version lors de l'approvisionnement ou
        à la suite d'une demande de mise à jour upgradeFromMgt. La valeur
        CompleteFromProvisioning(2) indique que la dernière mise à jour
        logicielle a été le résultat d'une divergence de version lors de
        l'approvisionnement. La valeur CompleteFromMgt(3) indique que la
        dernière mise à jour logicielle a été le résultat du réglage de l'objet
        docsDevSwAdminStatus à la valeur upgradeFromMgt. La valeur Failed(4)
        indique que la dernière tentative de téléchargement a échoué,
        ordinairement en raison d'une fin de temporisation TFTP."

     ::= { cabhSecFwBase 4 }


cabhSecFwPolicyFileCurrentVersion OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Version de l'ensemble de règles actuellement active dans le
       dispositif PS. Cet objet devrait être présenté dans la syntaxe utilisée
       par le vendeur individuel afin d'identifier les versions logicielles.
       Tout élément des services PS DOIT renvoyer une chaîne décrivant le
       fichier d'ensemble de règles actuellement chargé. Si cela n'est pas
       applicable, cet objet DOIT contenir une chaîne vide."
     ::= { cabhSecFwBase 5 }

--
--   Paramètres de journalisation du pare-feu
--

cabhSecFwEventType1Enable OBJECT-TYPE
SYNTAX    INTEGER {
          enable (1), -- journaliser l'événement
          disable (2) -- ne pas journaliser l'événement
          }
MAX-ACCESS read-write
STATUS current
DESCRIPTION
    "Cet objet active ou désactive la journalisation des messages d'événement
    de pare-feu de type 1. Les messages d'événement de type 1 signalent des
    tentatives, par des clients aussi bien privés que publics, de traverser
    le pare-feu qui violent la politique de sécurité."

DEFVAL { disable }
::= { cabhSecFwLogCtl 1 }

cabhSecFwEventType2Enable OBJECT-TYPE
SYNTAX    INTEGER {
          enable (1), -- journaliser l'événement
          disable (2) -- ne pas journaliser l'événement
          }
MAX-ACCESS read-write
STATUS current
DESCRIPTION
    "Cet objet active ou désactive la journalisation des messages d'événement
    de pare-feu de type 2. Les messages d'événement de type 2 signalent les
    tentatives d'attaque par refus de service identifiées."

DEFVAL { disable }
::= { cabhSecFwLogCtl 2 }
```

```
cabhSecFwEventType3Enable OBJECT-TYPE
SYNTAX INTEGER {
enable (1), -- journaliser l'événement
disable (2) -- ne pas journaliser l'événement
}
MAX-ACCESS read-write
STATUS current
DESCRIPTION
    "Active ou désactive la journalisation des messages d'événement de pare-feu
    de type 3. Les messages d'événement de type 3 signalent les changements
    apportés aux paramètres suivants de gestion de pare-feu:
    cabhSecFwPolicyFileURL, cabhSecFwPolicyFileCurrentVersion,
    cabhSecFwPolicyFileEnable."

DEFVAL { disable }
::= { cabhSecFwLogCtl 3 }

cabhSecFwEventAttackAlertThreshold  OBJECT-TYPE
     SYNTAX   INTEGER    (0..65535)
     MAX-ACCESS read-write
     STATUS current
     DESCRIPTION
        "Si le nombre d'attaques par piratage de type 1 ou 2 dépasse ce seuil
        dans la période définie par l'objet cabhSecFwEventAttackAlertPeriod,
        un message d'événement de pare-feu DOIT être journalisé avec le niveau
        de priorité 4."
DEFVAL { 65535 }
     ::= { cabhSecFwLogCtl 4 }


cabhSecFwEventAttackAlertPeriod OBJECT-TYPE
SYNTAX INTEGER (0..65535)
MAX-ACCESS read-write
STATUS current
DESCRIPTION
    "Indique la période à utiliser (en heures) pour le seuil
    cabhSecFwEventAttackAlertThreshold. Cette variable de base MIB devrait
    toujours garder trace des x dernières heures d'événements c'est-à-dire que
    si la variable est réglée de façon à suivre les événements pendant 10
    heures, alors, lorsque la 11e heure est atteinte, la 1re heure d'événements
    est supprimée du journal de suivi. Une valeur par défaut est mise à zéro
    de façon à indiquer l'heure zéro, de façon que cette variable de base MIB
    ne journalise aucun événement sauf configuration contraire."
DEFVAL {0}

::= { cabhSecFwLogCtl 5 }



cabhSecCertPsCert OBJECT-TYPE
SYNTAX    X509Certificate
MAX-ACCESS   read-only
STATUS    current
DESCRIPTION
    "Certificat X509 à codage DER du service portail."
REFERENCE
"Exigences de la section 11.3, Exigences (de sécurité) de la spécification"
::= { cabhSecCertObjects 1 }
```

```
--
-- Ce groupe de notifications fera l'objet d'extensions futures.
--

cabhSecNotification OBJECT IDENTIFIER ::= { cabhSecMib 3 0 }
cabhSecConformance  OBJECT IDENTIFIER ::= { cabhSecMib 4 }
cabhSecCompliances  OBJECT IDENTIFIER ::= { cabhSecConformance 1 }
cabhSecGroups       OBJECT IDENTIFIER ::= { cabhSecConformance 2 }

--
--    Groupe de notifications
--



-- déclarations de conformité

cabhSecBasicCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
       "Déclaration de conformité pour la capacité de pare-feu de réseau câblé."
    MODULE   --cabhSecMib







-- groupes inconditionnellement obligatoires

    MANDATORY-GROUPS {
            cabhSecGroup
    }

::= { cabhSecCompliances 3 }


cabhSecGroup OBJECT-GROUP
    OBJECTS {
       cabhSecFwPolicyFileEnable,
       cabhSecFwPolicyFileURL,
       cabhSecFwPolicyFileHash,
       cabhSecFwPolicyFileOperStatus,
       cabhSecFwPolicyFileCurrentVersion,

       cabhSecFwEventType1Enable,
       cabhSecFwEventType2Enable,
       cabhSecFwEventType3Enable,
       cabhSecFwEventAttackAlertThreshold,
       cabhSecFwEventAttackAlertPeriod,
       cabhSecCertPsCert
    }
    STATUS    current
    DESCRIPTION
        "Groupe d'objets contenus dans la base MIB du pare-feu de réseau câblé"
    ::= { cabhSecGroups 1 }

END
```

E.4 Définition

La base MIB de définition DOIT être implémentée comme défini ci-dessous.

```
CLAB-DEF-MIB DEFINITIONS ::= BEGIN
IMPORTS
     MODULE-IDENTITY,
     X509Certificate         FROM DOCS-BPI2-MIB
     enterprises        FROM SNMPv2-SMI;

cableLabs MODULE-IDENTITY
     LAST-UPDATED    "0209200000Z" -- 20 septembre, 2002
    ORGANIZATION    "CableLabs"
    CONTACT-INFO
            "Ralph Brown
            Adresse postale: Cable Television Laboratories, Inc.
                    400 Centennial Parkway
                    Louisville, Colorado 80027-1266
                    ETATS-UNIS D'AMÉRIQUE
            Tél.:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: r.brown@cablelabs.com"
    DESCRIPTION
        "Le présent module de base MIB fournit les catégories d'objets
        de gestion de base pour l'entreprise Cable Labs."

    ::= { enterprises 4491 }

clabFunction  OBJECT IDENTIFIER ::= { cableLabs 1 }
clabFuncMib2  OBJECT IDENTIFIER ::= { clabFunction 1 }
clabFuncProprietary OBJECT IDENTIFIER ::= { clabFunction 2 }
clabProject   OBJECT IDENTIFIER ::= { cableLabs 2 }
clabProjDocsis   OBJECT IDENTIFIER ::= { clabProject 1 }
clabProjPacketCable OBJECT IDENTIFIER ::= { clabProject 2 }
clabProjOpenCable  OBJECT IDENTIFIER ::= { clabProject 3}
clabProjCableHome   OBJECT IDENTIFIER ::= { clabProject 4 }
clabSecurity  OBJECT IDENTIFIER ::= { cableLabs 3}

clabSecCertObject OBJECT IDENTIFIER ::= { clabSecurity 1 }

clabSrvcPrvdrRootCACert     OBJECT-TYPE
    SYNTAX    X509Certificate
    MAX-ACCESS   read-only
    STATUS    current
    DESCRIPTION
        "Certificat CA racine de fournisseur de services X509 à
        codage selon les règles DER."
    REFERENCE
    "Section 11"
    ::= { clabSecCertObject 1 }

clabCVCRootCACert      OBJECT-TYPE
    SYNTAX    X509Certificate
    MAX-ACCESS   read-only
    STATUS    current
    DESCRIPTION
        "Certificat CA racine de CVC X509 à codage selon les règles DER."
    REFERENCE
    "Section 11 pour éléments de services PS autonomes seulement"
    ::= { clabSecCertObject 2 }
```

```
clabCVCCACert    OBJECT-TYPE
    SYNTAX    X509Certificate
    MAX-ACCESS   read-only
    STATUS    current
    DESCRIPTION
        "Certificat CA de CVC X509 à codage selon les règles DER du
        laboratoire CableLabs."
    REFERENCE
    "Section 11 pour éléments de services PS autonomes seulement"
    ::= { clabSecCertObject 3 }

clabMfgCVCCert     OBJECT-TYPE
    SYNTAX    X509Certificate
    MAX-ACCESS   read-only
    STATUS    current
    DESCRIPTION
        "Certificat de CVC de constructeur X509 à codage selon les règles DER."
    REFERENCE
    "Section 11 pour éléments de services PS autonomes seulement"
    ::= { clabSecCertObject 4 }

END
```

E.5 Base MIB de portail DHCP du câble (CDP)

La base MIB de portail CDP DOIT être implémentée comme défini ci-dessous.

```
CABH-CDP-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
     Integer32,
     Unsigned32
                    FROM SNMPv2-SMI
     TruthValue,
     TimeStamp,
     RowStatus,
    TEXTUAL-CONVENTION
                    FROM SNMPv2-TC
    OBJECT-GROUP,
    MODULE-COMPLIANCE
                    FROM SNMPv2-CONF
    InetAddressType,
    InetAddress,
    InetAddressIPv4,
    InetAddressIPv6
                       FROM INET-ADDRESS-MIB
     SnmpAdminString         FROM SNMP-FRAMEWORK-MIB -- RFC 2571
    clabProjCableHome
                    FROM CLAB-DEF-MIB;

--============================================================================
--
--   Historique:
--
--   Date      Modifié par        Raison
--
--============================================================================

cabhCdpMib MODULE-IDENTITY
    LAST-UPDATED    "0209200000Z" -- 20 septembre, 2002
    ORGANIZATION    "CableLabs Broadband Access Department"
```

```
    CONTACT-INFO
            "Kevin Luehrs
            Adresse postale: Cable Television Laboratories, Inc.
                    400 Centennial Parkway
                    Louisville, Colorado 80027-1266
                    ETATS-UNIS D'AMÉRIQUE
            Tél.:   +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
        "Le présent module de base MIB fournit les objets de gestion de
        base pour la portion relative au portail DHCP du câble (CDP) de
        la base de données MIB du service PS.



    ::=  { clabProjCableHome 4 }

-- Conventions textuelles
CabhCdpLanTransDhcpClientId ::= TEXTUAL-CONVENTION
     STATUS   current
     DESCRIPTION
          "Informations d'option DHCP 61 de secteur LAN-Trans."
     SYNTAX OCTET STRING (SIZE (1..80))


cabhCdpObjects   OBJECT IDENTIFIER ::= { cabhCdpMib 1 }
cabhCdpBase      OBJECT IDENTIFIER ::= { cabhCdpObjects 1 }
cabhCdpAddr      OBJECT IDENTIFIER ::= { cabhCdpObjects 2 }
cabhCdpServer    OBJECT IDENTIFIER ::= { cabhCdpObjects 3 }
--
--   Le groupe suivant décrit les objets de base contenus dans le portail DHCP
--   par câble. Le reste de ce groupe traite les adresses définies du côté LAN.

cabhCdpSetToFactory     OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Le fait de mettre cet objet à la valeur true(1) provoque le retour
        des options DHCP par défaut aux valeurs par défaut de l'usine. La
        lecture de cet objet renvoie toujours la valeur false(2). Lorsque
        l'objet cabhCdpSetToFactory est réglé à la valeur true, les actions
        suivantes ont lieu:
        1. effacement de toutes les entrées d'objet cabhCdpLanAddr dans la
        table d'adresses LAN du portail CDP.
        2. retour de toutes les options DHCP de serveur CDS aux valeurs par
        défaut de l'usine.
        3. offre des options DHCP par défaut de l'usine par le serveur CDS à
        la prochaine échéance de renouvellement de location.
        Les objets réglés aux valeurs par défaut de l'usine sont les suivants:
      cabhCdpLanTransThreshold,
      cabhCdpLanTransAction,
      cabhCdpWanDataIpAddrCount,
      cabhCdpLanStartType,
      cabhCdpLanPoolStart,
      cabhCdpLanPoolEndType,
      cabhCdpLanPoolEnd,
      cabhCdpNetworkNumber,
      cabhCdpServerSubnetMaskType,
      cabhCdpServerSubnetMask,
      cabhCdpServerTimeOffset,
      cabhCdpServerRouterType,
      cabhCdpServerRouter,
```

```
       cabhCdpServerDnsAddressType,
       cabhCdpServerDnsAddress,
       cabhCdpServerSyslogAddressType,
       cabhCdpServerSyslogAddress,
       cabhCdpServerDomainName,
       cabhCdpServerTTL,
       cabhCdpServerInterfaceMTU,
       cabhCdpServerVendorSpecific,
       cabhCdpServerLeaseTime,
       cabhCdpServerDhcpAddressType,
       cabhCdpServerDhcpAddress"
REFERENCE
""
::= { cabhCdpBase 1 }



cabhCdpLanTransCurCount OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
        "Nombre actuel d'adresses IP de secteur LAN-Trans pour adresses
        traduites (par interconnexion des traductions NAT et NAPT). C'est
        un décompte des adresses du côté LAN."
     REFERENCE
       ""
    ::= { cabhCdpBase 2 }

cabhCdpLanTransThreshold OBJECT-TYPE
    SYNTAX      INTEGER (0..65533)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Seuil numérique des adresses IP de secteur LAN-Trans attribuées ou
        assignées au-dessus duquel le service PS produit une condition d'alarme.
        Un événement est produit chaque fois que l'on essaie d'attribuer une
        adresse IP de secteur LAN-Trans alors que la valeur de l'objet
        cabhCdpLanTransCurCount est supérieure ou égale à celle de l'objet
        cabhCdpLanTransThreshold. Une valeur de 0 indique que le portail CDP
        règle le seuil au plus grand nombre d'adresses contenues dans la réserve
        d'adresses de réseau LAN."

     DEFVAL { 0 }
    ::= { cabhCdpBase 3 }

cabhCdpLanTransAction OBJECT-TYPE
    SYNTAX      INTEGER {
     normal    (1),
     noAssignment  (2)
     }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Action qui a lieu lorsque le serveur CDS assigne une adresse de secteur
        LAN-Trans et lorsque le nombre d'adresses de secteur LAN-Trans assignées
        (objet cabhCdpLanTransCurCount) est supérieur au seuil (objet
        cabhCdpLanTransThreshold). Cette action est la suivante:

              normal – assigner une adresse IP de secteur LAN-Trans et
              traiter l'interconnexion entre les réseaux LAN et WAN comme
              cela serait normalement le cas si le seuil n'avait pas été
              dépassé.
```

```
                noAssignment - ne pas assigner d'adresse IP de secteur LAN-Trans
                et ne pas créer d'interconnexion."
     REFERENCE
       ""
     DEFVAL { normal }
    ::= { cabhCdpBase 4 }

cabhCdpWanDataIpAddrCount OBJECT-TYPE
    SYNTAX      INTEGER ( 0..63 )
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Nombre d'adresses IP de réseau WAN-Data que le client CDC a besoin
        d'acquérir en DHCP."

     REFERENCE
       ""
     DEFVAL { 0 }
    ::= { cabhCdpBase 5 }

--
--   Tables de gestion d'adresses du portail CDP
--
--========================================================================
--
--   cabhCdpLanAddrTable (table d'adresses LAN du portail CDP)
--
--   L'objet cabhCdpLanAddrTable contient les paramètres DHCP
--   pour chaque adresse IP servie au secteur LAN-Trans.
--
--   Cette table contient une liste des entrées pour les paramètres de portail
--   CDP du côté LAN.
--   Ces  paramètres peuvent être réglés  soit par le portail CDP ou par le
--   câblo-opérateur au moyen du portail CMP.
========================================================================

cabhCdpLanAddrTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCdpLanAddrEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Cette table est une liste de paramètres du secteur LAN-Trans. Cette
        liste possède une entrée pour chaque adresse IP de secteur LAN-Trans
        attribuée."
    ::= {  cabhCdpAddr 1 }

cabhCdpLanAddrEntry OBJECT-TYPE
    SYNTAX      CabhCdpLanAddrEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Liste de paramètres généraux pour mappages de portail CDP."
    INDEX { cabhCdpLanAddrIpType, cabhCdpLanAddrIp }
    ::= { cabhCdpLanAddrTable 1 }

CabhCdpLanAddrEntry ::= SEQUENCE {
cabhCdpLanAddrIpType             InetAddressType,
     cabhCdpLanAddrIp            InetAddress,
     cabhCdpLanAddrClientID           CabhCdpLanTransDhcpClientId,
     cabhCdpLanAddrLeaseCreateTime        TimeStamp,
     cabhCdpLanAddrLeaseExpireTime        TimeStamp,
     cabhCdpLanAddrMethod            INTEGER,
     cabhCdpLanAddrHostName      SnmpAdminString,
     cabhCdpLanAddrRowStatus     RowStatus
    }
```

```
cabhCdpLanAddrIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Type d'adresse assignée du côté LAN pour la table d'adresses du
        portail CDP."
    DEFVAL  { ipv4 }
    ::= { cabhCdpLanAddrEntry 1 }



cabhCdpLanAddrIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Adresse assignée du côté LAN pour la table d'adresses de portail CDP.
        Ce paramètre est introduit par le portail CDP lorsque le serveur CDS
        accorde une location à un dispositif IP de réseau LAN dans le secteur
        LAN-Trans et crée une rangée dans cette table. En variante, ce paramètre
        peut être créé par le système NMS par l'intermédiaire du portail CMP,
        lorsque le système NMS crée une nouvelle réservation d'adresse DHCP en
        accédant à l'objet cabhCdpLanAddrRowStatus avec un index composé d'une
        nouvelle adresse cabhCdpLanAddrIp et de son type."

    ::= { cabhCdpLanAddrEntry 2 }

cabhCdpLanAddrClientID OBJECT-TYPE
    SYNTAX      CabhCdpLanTransDhcpClientId
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
        "Identificateur de client tel qu'indiqué dans l'option 61 du message
        DHCP DISCOVER. Il y a relation univoque entre l'identificateur de
        client et l'adresse LAN assignée. Ce paramètre est introduit par le
        portail CDP lorsque le serveur CDS accorde une location à un dispositif
        IP de réseau LAN dans le secteur LAN Trans et crée une rangée dans
        cette table. En variante, ce paramètre peut être créé par le système
        NMS par l'intermédiaire du portail CMP lorsque le système NMS crée une
        nouvelle réservation d'adresse DHCP en accédant à l'objet
        cabhCdpLanDataAddrRowStatus avec un index composé d'une nouvelle
        adresse cabhCdpLanAddrIp et d'un nouvel identificateur
        cabhCdpLanAddrClientID."

    ::= { cabhCdpLanAddrEntry 3 }

cabhCdpLanAddrLeaseCreateTime OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Instant auquel a été créé le côté LAN de la table de réseau LAN
       du portail CDP. Cette entrée n'est  réglée que lorsque l'objet
       cabhCdpLanAddrTable est créé et que cette entrée n'existe pas
       encore. En d'autres termes, cette valeur n'est pas récrite au moment
       du renouvellement de la location."
    ::= { cabhCdpLanAddrEntry 4 }

cabhCdpLanAddrLeaseExpireTime OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
       "Instant auquel la location du côté LAN arrive à expiration. A ce moment,
       cette entrée est supprimée de la table."
    ::= { cabhCdpLanAddrEntry 5 }

cabhCdpLanAddrMethod OBJECT-TYPE
    SYNTAX      INTEGER {
     cmp (1),
     cdp (2)
     }
     MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Méthode de création de cette entrée d'adresse. La valeur 'cmp'
       indique que cette rangée (entrée) a été configurée par l'intermédiaire
       du portail CMP. La valeur 'cdp' indique que c'est un message DHCP
       DISCOVER qui a établi cette rangée (entrée)."
    ::= { cabhCdpLanAddrEntry 6 }

cabhCdpLanAddrHostName OBJECT-TYPE
    SYNTAX      SnmpAdminString(SIZE(0..80))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Nom du serveur de l'adresse IP du réseau LAN, sur la base de l'option 12
       du protocole DHCP."
    ::= { cabhCdpLanAddrEntry 7 }


cabhCdpLanAddrRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "Verrouillage de rangée pour création et suppression."
    ::= { cabhCdpLanAddrEntry 8 }


--============================================================================
--
--   Objet cabhCdpWanDataAddrTable (Table d'adresses de réseau WAN-Data du
--   portail CDP)
--
--   L'objet cabhCdpWanDataAddrTable contient les paramètres de configuration
--   ou DHCP pour chaque mappage d'adresse IP sur une adresse IP de
--   réseau WAN-Data.
--
--============================================================================

cabhCdpWanDataAddrTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCdpWanDataAddrEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "Cette table contient des informations de secteur d'adresses de réseau
       WAN-Data."
    ::= {  cabhCdpAddr 2 }

cabhCdpWanDataAddrEntry OBJECT-TYPE
    SYNTAX      CabhCdpWanDataAddrEntry
    MAX-ACCESS  not-accessible
    STATUS      current
```

```
    DESCRIPTION
        "Liste de paramètres généraux pour secteur d'adresses de réseau WAN-Data
        de portail CDP."
    INDEX { cabhCdpWanDataAddrIndex }
    ::= { cabhCdpWanDataAddrTable 1 }

CabhCdpWanDataAddrEntry ::= SEQUENCE {
     cabhCdpWanDataAddrIndex      INTEGER,
     cabhCdpWanDataAddrClientId       OCTET STRING,
     cabhCdpWanDataAddrIpType         InetAddressType,
     cabhCdpWanDataAddrIp             InetAddress,
     cabhCdpWanDataAddrRenewalTime    Integer32,
     cabhCdpWanDataAddrRowStatus      RowStatus
    }


cabhCdpWanDataAddrIndex OBJECT-TYPE
    SYNTAX      INTEGER (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "Index de pointage dans la table."
    ::= { cabhCdpWanDataAddrEntry 1 }

cabhCdpWanDataAddrClientId OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE (1..80))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "Identificateur unique de client de réseau WAN-Data utilisé lors d'une
       tentative d'acquisition d'une adresse IP de réseau WAN-Data via DHCP."
    ::= { cabhCdpWanDataAddrEntry 2 }

cabhCdpWanDataAddrIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Type d'adresse assignée du côté WAN-Data."
    DEFVAL { ipv4 }
    ::= { cabhCdpWanDataAddrEntry 3 }

cabhCdpWanDataAddrIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Adresse assignée du côté WAN-Data."
    ::= { cabhCdpWanDataAddrEntry 4 }

cabhCdpWanDataAddrRenewalTime OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Durée restant avant l'expiration de la location. Valeur fondée
       sur l'option DHCP 51."
    ::= { cabhCdpWanDataAddrEntry 5 }

cabhCdpWanDataAddrRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
```

```
    DESCRIPTION
       "Verrouillage d'état de rangée pour création et suppression."
    ::= { cabhCdpWanDataAddrEntry 6 }

--============================================================================
--
--   Objet cabhCdpWanDataAddrServerTable (Table de serveur DNS du
--   réseau WAN-Data)
--
--   L'objet cabhCdpWanDataAddrServerTable contient une table de serveurs DNS
--   de référence.
--
--============================================================================

cabhCdpWanDataAddrServerTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCdpWanDataAddrServerEntry
     MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Cette table contient les adresses IP utilisées pour les serveurs DNS
        du réseau WAN-Data. Ces adresses sont obtenues via l'option DHCP 6
        pendant le processus WAN-Data."
    ::= {  cabhCdpAddr 3 }

cabhCdpWanDataAddrServerEntry OBJECT-TYPE
    SYNTAX      CabhCdpWanDataAddrServerEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Liste de serveurs DNS du réseau WAN-Data."
    INDEX { cabhCdpWanDataAddrDnsIpType, cabhCdpWanDataAddrDnsIp }
    ::= { cabhCdpWanDataAddrServerTable 1 }

CabhCdpWanDataAddrServerEntry ::= SEQUENCE {
    cabhCdpWanDataAddrDnsIpType  InetAddressType,
    cabhCdpWanDataAddrDnsIp      InetAddress,
    cabhCdpWanDataAddrDnsRowStatus    RowStatus
    }


cabhCdpWanDataAddrDnsIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Ce paramètre indique le type d'adresse IP d'un serveur DNS."
     DEFVAL  { ipv4 }
     ::= { cabhCdpWanDataAddrServerEntry 1 }


cabhCdpWanDataAddrDnsIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Ce paramètre indique l'adresse IP d'un serveur DNS."
     ::= { cabhCdpWanDataAddrServerEntry 2 }

cabhCdpWanDataAddrDnsRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
```

```
    DESCRIPTION
       "Verrouillage d'état de rangée pour création et suppression."
     ::= { cabhCdpWanDataAddrServerEntry 3 }


--
--   Valeurs d'option du serveur DHCP du câble (CDS) pour le secteur LAN-Trans
--

cabhCdpLanPoolStartType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Type d'adresse du début de liste d'adresses IP de secteur LAN Trans."
     DEFVAL { ipv4 }
    ::= { cabhCdpServer 1 }

cabhCdpLanPoolStart OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Début de liste d'adresses IP de secteur LAN Trans."
     DEFVAL { 'c0a8000a'h }  -- 192.168.0.10
     -- 192.168.0.0 est le numéro du réseau
     -- 192.168.0.255 est la diffusion
     -- l'adresse et le numéro 192.168.0.1
     -- sont réservés pour le routeur
    ::= { cabhCdpServer 2 }

cabhCdpLanPoolEndType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Type d'adresse type de la fin de liste d'adresses de secteur LAN Trans."
     DEFVAL { ipv4 }
    ::= { cabhCdpServer 3 }

cabhCdpLanPoolEnd OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Fin de liste d'adresses IP de secteur LAN-Trans."
     DEFVAL { 'c0a800fe'h }  -- 192.168.0.254
    ::= { cabhCdpServer 4 }

cabhCdpServerNetworkNumberType   OBJECT-TYPE
     SYNTAX    InetAddressType
MAX-ACCESS   read-write
STATUS    current
DESCRIPTION
   "Type d'adresse IP du numéro de réseau dans le secteur LAN-Trans."
DEFVAL  { ipv4 }
::= { cabhCdpServer 5 }

cabhCdpServerNetworkNumber       OBJECT-TYPE
SYNTAX    InetAddress
MAX-ACCESS   read-write
STATUS    current
```

```
DESCRIPTION
    "Numéro de réseau dans le secteur LAN-Trans."
DEFVAL  { 'c0a80000'h }
::= { cabhCdpServer 6 }



cabhCdpServerSubnetMaskType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Type de masque de sous-réseau dans le secteur LAN-Trans."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 7 }

cabhCdpServerSubnetMask OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Valeur d'option 1 – valeur du masque de sous-réseau du
       secteur LAN-Trans."
     DEFVAL { 'ffffff00'h }  -- 255.255.255.0
    ::= { cabhCdpServer 8 }

cabhCdpServerTimeOffset OBJECT-TYPE
    SYNTAX      Integer32 (-86400..86400)  -- 0 à 24 h (en secondes)
    UNITS "secondes"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Valeur d'option 2 – valeur de décalage temporel du secteur LAN-Trans
       par rapport au temps universel coordonné (UTC)."
     DEFVAL { 0 }  -- UTC
    ::= { cabhCdpServer 9 }

cabhCdpServerRouterType OBJECT-TYPE
     SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Type d'adresse, Routeur pour le secteur d'adresse LAN-Trans
     DEFVAL { ipv4 }
    ::= { cabhCdpServer 10 }

cabhCdpServerRouter    OBJECT-TYPE
     SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Valeur d'option 3 – Routeur pour le secteur d'adresse LAN-Trans
     DEFVAL { 'c0a80001'h }  -- 192.168.0.1
    ::= { cabhCdpServer 11 }

cabhCdpServerDnsAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Type d'adresses IP du secteur d'adresses LAN-Trans de serveur DNS."
     DEFVAL { ipv4 }
    ::= { cabhCdpServer 12 }
```

```
cabhCdpServerDnsAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Adresse IP des serveurs DNS du secteur d'adresses LAN-Trans. Par
       défaut il n'y a qu'un seul serveur DNS et c'est l'adresse spécifiée
       dans la valeur d'option 3 – objet cabhCdpServerRouter. Une seule
       adresse est spécifiée. DNS servers."
     DEFVAL { ipv4 }
    ::= { cabhCdpServer 12 }

cabhCdpServerDnsAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Type d'adresse IP des serveurs d'enregistrement SYSLOG du
       secteur LAN-Trans."
     DEFVAL { ipv4 }
    ::= { cabhCdpServer 14 }

cabhCdpServerSyslogAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Adresses IP des serveurs d'enregistrement SYSLOG du secteur LAN-Trans.
       Par défaut, il n'y a pas de serveur d'enregistrement. Les valeurs par
       défaut de l'usine contiennent l'indication que la valeur d'absence de
       serveur d'enregistrement est égale à (0.0.0.0)."
     DEFVAL { '00000000'h }  -- 0.0.0.0
    ::= { cabhCdpServer 15 }

cabhCdpServerDomainName OBJECT-TYPE
    SYNTAX      SnmpAdminString(SIZE(0..128))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Valeur d'option 15 – Nom de domaine du secteur d'adresses LAN-Trans."
     DEFVAL {""}
     ::= { cabhCdpServer 16 }

cabhCdpServerTTL OBJECT-TYPE
     SYNTAX      INTEGER (0..255)
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Valeur d'option 23 – Temps de recherche de relais dans le
        secteur LAN-Trans."
     DEFVAL  { 64 }
     ::= { cabhCdpServer 17 }

cabhCdpServerInterfaceMTU   OBJECT-TYPE
     SYNTAX      INTEGER (68..4096)
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Valeur d'option 26 – Unité MTU d'interface dans le secteur LAN-Trans."
     ::= { cabhCdpServer 18 }

cabhCdpServerVendorSpecific  OBJECT-TYPE
     SYNTAX      OCTET STRING (SIZE(0..255))
     MAX-ACCESS  read-write
```

```
    STATUS      current
    DESCRIPTION
        "Valeur d'option 43 – Options spécifiques du vendeur."
     DEFVAL  { ''h }
     ::= { cabhCdpServer 19 }

cabhCdpServerLeaseTime  OBJECT-TYPE
     SYNTAX      Unsigned32
     UNITS    "secondes"
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Valeur d'option 51 – Durée de location pour dispositifs IP de réseau
        LAN dans le secteur LAN-Trans (en secondes)."
DEFVAL  { 3600 }

     ::= { cabhCdpServer 20 }

cabhCdpServerDhcpAddressType OBJECT-TYPE
     SYNTAX      InetAddressType
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Valeur d'option 54 – Type d'adresse IP du serveur DHCP dans le
        secteur LAN-Trans."
     DEFVAL { ipv4 }
     ::= { cabhCdpServer 21 }

cabhCdpServerDhcpAddress    OBJECT-TYPE
     SYNTAX      InetAddress
     MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Valeur d'option 54 – Adresse IP du serveur DHCP dans le secteur
       LAN-Trans. Sa valeur par défaut est celle du routeur adresse comme
       spécifié dans l'objet cabhCdpServerRouter. En variante, un vendeur
       PEUT décider de séparer l'adresse du serveur CDS de celle du routeur."
     DEFVAL { 'c0a80001'h }      --   192.168.0.1
     ::= { cabhCdpServer 22 }


--
-- Ce groupe de notifications fera l'objet d'extensions futures.
--

cabhCdpNotification OBJECT IDENTIFIER ::= { cabhCdpMib 2 0 }
cabhCdpConformance  OBJECT IDENTIFIER ::= { cabhCdpMib 3 }
cabhCdpCompliances  OBJECT IDENTIFIER ::= { cabhCdpConformance 1 }
cabhCdpGroups       OBJECT IDENTIFIER ::= { cabhCdpConformance 2 }

--
--    Groupe de notifications
--


-- déclarations de conformité

cabhCdpBasicCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
       "Déclaration de conformité des dispositifs qui implémentent un
       adaptateur MTA."
    MODULE   --cabhCdpMib
```

```
-- groupes inconditionnellement obligatoires

    MANDATORY-GROUPS {
            cabhCdpGroup
    }

::= { cabhCdpCompliances 3 }


cabhCdpGroup  OBJECT-GROUP

  OBJECTS {

cabhCdpSetToFactory,
cabhCdpLanTransCurCount,
cabhCdpLanTransThreshold,
cabhCdpLanTransAction,
cabhCdpWanDataIpAddrCount,

cabhCdpLanAddrClientID,
cabhCdpLanAddrLeaseCreateTime,
cabhCdpLanAddrLeaseExpireTime,
cabhCdpLanAddrMethod,
cabhCdpLanAddrHostName,
cabhCdpLanAddrRowStatus,

cabhCdpWanDataAddrClientId,
cabhCdpWanDataAddrIp,
cabhCdpWanDataAddrRenewalTime,
cabhCdpWanDataAddrRowStatus,

cabhCdpWanDataAddrDnsRowStatus,

cabhCdpLanPoolStartType,
cabhCdpLanPoolStart,
cabhCdpLanPoolEndType,
cabhCdpLanPoolEnd,
cabhCdpServerNetworkNumberType,
cabhCdpServerNetworkNumber,
cabhCdpServerSubnetMaskType,
cabhCdpServerSubnetMask,
cabhCdpServerTimeOffset,


cabhCdpServerRouterType,
cabhCdpServerRouter,
cabhCdpServerDnsAddressType,
cabhCdpServerDnsAddress,
cabhCdpServerSyslogAddressType,
cabhCdpServerSyslogAddress,
cabhCdpServerDomainName,
cabhCdpServerTTL,
cabhCdpServerInterfaceMTU,
cabhCdpServerVendorSpecific,
cabhCdpServerLeaseTime,
cabhCdpServerDhcpAddressType,
cabhCdpServerDhcpAddress
       }
    STATUS    current
    DESCRIPTION
       "Groupe d'objets pour base MIB de portail CDP de réseau câblé."
    ::= { cabhCdpGroups 1 }

END
```

E.6 Portail d'adresse câble (CAP)

La base MIB du portail CAP DOIT être implémentée comme défini ci-dessous.

```
CABH-CAP-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
      Unsigned32
          FROM SNMPv2-SMI
      TimeStamp,
      TruthValue,
      RowStatus,
      PhysAddress
          FROM SNMPv2-TC
    OBJECT-GROUP,
    MODULE-COMPLIANCE   FROM SNMPv2-CONF
    InetAddressType,
    InetAddress,
    InetAddressIPv4,
    InetAddressIPv6          FROM INET-ADDRESS-MIB
    clabProjCableHome
          FROM CLAB-DEF-MIB;

--============================================================================
--
--   Historique:
--
--   Date      Modifié par   Raison
--
--
--============================================================================

cabhCapMib MODULE-IDENTITY
    LAST-UPDATED    "0209200000Z" -- 20 septembre, 2002
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Adresse postale: Cable Television Laboratories, Inc.
                   400 Centennial Parkway
                   Louisville, Colorado 80027-1266
                   ETATS-UNIS D'AMÉRIQUE
            Tél:    +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
       "Le présent module de base MIB fournit les objets de gestion de base
       pour la portion de portail d'adresse câble (CAP) de la base de données
       MIB du service PS."



    ::=  { clabProjCableHome 3 }

-- Conventions textuelles

CabhCapPacketMode ::= TEXTUAL-CONVENTION
     STATUS   current
     DESCRIPTION
        "Type de données établi lorsqu'une association ou un mappage est
        établi."
```

```
     SYNTAX   INTEGER {
                  napt      (1), -- Traduction NAT de point d'accès
                  nat       (2), -- Traduction NAT de base
                  passthrough   (3)  -- Adresse externe de traversée
                  }


cabhCapObjects      OBJECT IDENTIFIER ::= { cabhCapMib 1 }
cabhCapBase         OBJECT IDENTIFIER ::= { cabhCapObjects 1 }
cabhCapMap           OBJECT IDENTIFIER ::= { cabhCapObjects 2 }


--=================================================================
--
--   Paramètres généraux de portail CAP
--
--=================================================================

cabhCapTcpTimeWait OBJECT-TYPE
    SYNTAX Unsigned32
    UNITS "secondes"
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
       "Cet objet indique la durée maximale d'inactivité à attendre avant de
       considérer que la session de protocole TCP est terminée. Il ne possède
       aucune relation avec l'état d'attente TIME_WAIT de session TCP auquel
       il est fait référence dans [RFC 793]."
    DEFVAL { 300 }
    ::= { cabhCapBase 1 }


cabhCapUdpTimeWait OBJECT-TYPE
     SYNTAX      Unsigned32
     UNITS    "secondes"
     MAX-ACCESS  read-write
     STATUS      current
     DESCRIPTION
        "Durée d'inactivité à attendre avant de détruire les mappages CAP
        pour UDP."
     DEFVAL { 300 }  -- 5 minutes
     ::={ cabhCapBase 2 }

cabhCapIcmpTimeWait OBJECT-TYPE
     SYNTAX      Unsigned32
     UNITS "secondes"
     MAX-ACCESS read-write
     STATUS current
     DESCRIPTION
        "Durée d'inactivité à attendre avant de détruire les mappages
        CAP pour ICMP."
     DEFVAL { 300 }  --  5 minutes
     ::= { cabhCapBase 3 }


cabhCapPrimaryMode OBJECT-TYPE
    SYNTAX   CabhCapPacketMode
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Mode de traitement primaire de paquet à utiliser."
    DEFVAL { napt }
    ::= { cabhCapBase 4 }
```

```
cabhCapSetToFactory OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
       "Le fait de mettre cet objet à la valeur true(1) provoque l'effacement
       de toutes les tables contenues dans le portail CAP, et le retour de
       tous les objets de portail CAP à leurs valeurs par défaut s'ils en ont.

       Les objets à mettre aux valeurs par défaut de l'usine lorsqu'ils sont mis
       à la valeur 'true' sont énumérés ci-dessous:
         cabhCapTcpTimeWait,
         cabhCapUdpTimeWait,
         cabhCapIcmpTimeWait,
         cabhCapPrimaryMode,
         cabhCapMappingWanAddrType,
         cabhCapMappingWanPort,
         cabhCapMappingLanAddrType,
         cabhCapMappingLanPort."
    ::= { cabhCapBase 5 }


--------------------------------------------------------------------------
--
--   Objet cabhCapMappingTable (table de mappage du portail CAP)
--
--   Le cabhCapMappingTable contient les mappages pour tous les mappages de
--   portail CAP.
--
--------------------------------------------------------------------------

cabhCapMappingTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCapMappingEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "Cette table contient le mappage d'adresse IP pour tous les mappages de
       portail CAP."
    ::= {  cabhCapMap 1 }

cabhCapMappingEntry OBJECT-TYPE
    SYNTAX      CabhCapMappingEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
        "Liste des mappages d'adresse IP du portail CAP."
    INDEX { cabhCapMappingIndex }
    ::= { cabhCapMappingTable 1 }

     CabhCapMappingEntry ::= SEQUENCE {
     cabhCapMappingWanAddrType        InetAddressType,
     cabhCapMappingIndex              INTEGER,
     cabhCapMappingWanAddr            InetAddress,
     cabhCapMappingWanPort            INTEGER,
     cabhCapMappingLanAddrType        InetAddressType,
     cabhCapMappingLanAddr            InetAddress,
     cabhCapMappingLanPort            INTEGER,
     cabhCapMappingMethod             INTEGER,
     cabhCapMappingProtocol           INTEGER,
     cabhCapMappingRowStatus          RowStatus
     }
```

```
cabhCapMappingIndex    OBJECT-TYPE
    SYNTAX              INTEGER   (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "L'index d'entrée dans la table de mappage du portail CAP."
    ::= { cabhCapMappingEntry 1 }

cabhCapMappingWanAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "Type d'adresse IP assignée du côté WAN. La version IP 4 est normalement
       utilisée."
    DEFVAL { ipv4 }
    ::= { cabhCapMappingEntry 2 }

cabhCapMappingWanAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "Adresse IP assignée du côté WAN. La version IP 4 est normalement
       utilisée."
    ::= { cabhCapMappingEntry 3 }

cabhCapMappingWanPort OBJECT-TYPE
    SYNTAX      INTEGER (0..65535)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "Numéro de point d'accès en protocole TCP/UDP du côté WAN."
        DEFVAL { 0 }
    ::= { cabhCapMappingEntry 4 }

cabhCapMappingLanAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "Type d'adresse IP assignée du côté LAN. La version IP 4 est normalement
       utilisée."
    DEFVAL { ipv4 }
    ::= { cabhCapMappingEntry 5 }

cabhCapMappingLanAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "Adresse IP assignée du côté LAN. La version IP 4 est normalement
       utilisée."
    ::= { cabhCapMappingEntry 6 }

cabhCapMappingLanPort OBJECT-TYPE
    SYNTAX      INTEGER (0..65535)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "Numéro de point d'accès en protocole TCP/UDP du côté LAN."
    DEFVAL { 0 }
    ::= { cabhCapMappingEntry 7 }
```

```
cabhCapMappingMethod OBJECT-TYPE
    SYNTAX      INTEGER {
       static   (1),
       dynamic (2)
       }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
       "Cet objet indique comment ce mappage a été créé. La valeur 'static'
       signifie qu'il a été approvisionné, et la valeur 'dynamic' signifie
       qu'il a été manipulé par le service PS proprement dit."
    ::= { cabhCapMappingEntry 8 }

cabhCapMappingProtocol OBJECT-TYPE
    SYNTAX      INTEGER {
       other   (1), -- non spécifié
       icmp    (2),
       udp    (3),
       tcp    (4)
          }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "Protocole pour ce mappage."
    ::= { cabhCapMappingEntry 9 }

cabhCapMappingRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "Verrouillage d'état de rangée pour création et suppression d'une entrée
       d'objet cabhCapMappingTable. La modification de la valeur des colonnes
       d'adresse IP ou de numéro de point d'accès dans la table de mappage du
       portail CAP peut avoir une incidence sur le trafic actif, de sorte que
       le portail CMP empêchera la modification des colonnes de cette table
       lorsque l'objet cabhCapMappingRowStatus est dans l'état actif."
    ::={ cabhCapMappingEntry 10 }


================================================================================
--
--   Objet cabhCapPassthroughTable (Table de traversée du portail CAP)
--
--   L'objet cabhCapPassthroughTable contient les adresses de commande MAC
--   pour tous les dispositifs IP de réseau LAN, qui seront configurés en
--   mode de traversée.
--
================================================================================

cabhCapPassthroughTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCapPassthroughEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
       "Cette table contient des adresses MAC pour dispositifs IP de réseau LAN
       qui sont configurés en mode de traversée."
    ::= {  cabhCapMap 2 }

cabhCapPassthroughEntry OBJECT-TYPE
    SYNTAX   CabhCapPassthroughEntry
    MAX-ACCESSnot-accessible
    STATUS   current
```

```
    DESCRIPTION
       "Liste des adresses matérielles des dispositifs IP de réseau LAN qui
       sont configurés en mode de traversée."
    INDEX {cabhCapPassthroughIndex}
::= {cabhCapPassthroughTable 1}

CabhCapPassthroughEntry::=SEQUENCE {
     cabhCapPassthroughIndex     INTEGER,
     cabhCapPassthroughMacAddr   PhysAddress,
     cabhCapPassthroughRowStatus RowStatus
     }

cabhCapPassthroughIndex     OBJECT-TYPE
    SYNTAX   INTEGER (1..65535)
    MAX-ACCESSnot-accessible
    STATUS   current
    DESCRIPTION
        "Index d'entrée dans la table de traversée du portail CAP."
    ::= { cabhCapPassthroughEntry 1 }

cabhCapPassthroughMacAddr        OBJECT-TYPE
    SYNTAX   PhysAddress
    MAX-ACCESSread-create
    STATUS   current
    DESCRIPTION
       "Adresse matérielle du dispositif IP de réseau LAN à configurer en mode
       de traversée."
    ::={cabhCapPassthroughEntry 2}

cabhCapPassthroughRowStatus OBJECT-TYPE
    SYNTAX   RowStatus
    MAX-ACCESSread-create
    STATUS    current
    DESCRIPTION
       "Verrouillage d'état de rangée pour création et suppression d'une entrée
       dans l'objet cabhCapPassthroughTable. Il n'y a pas de restrictions
       concernant le réglage de la colonne de lecture-création de cette table
       (c'est-à-dire de l'objet cabhCapPassthroughMacAddr)lorsque l'objet
       cabhCapPassthroughRowStatus est à l'état actif."
    ::= { cabhCapPassthroughEntry 3 }

--
-- Ce groupe de notifications fera l'objet d'extensions futures.
--

cabhCapNotification     OBJECT IDENTIFIER ::= { cabhCapMib 2 0 }
cabhCapConformance OBJECT IDENTIFIER ::= { cabhCapMib 3 }
cabhCapCompliances OBJECT IDENTIFIER ::= { cabhCapConformance 1 }
cabhCapGroups OBJECT IDENTIFIER ::= { cabhCapConformance 2 }

--
--    Groupe de notifications
--


-- déclarations de conformité

cabhCapBasicCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
       "Déclaration de conformité des dispositifs qui implémentent
       l'adaptateur MTA."
    MODULE   --cabhCapMib
```

```
-- groupes inconditionnellement obligatoires

MANDATORY-GROUPS {
    cabhCapGroup
    }

::= { cabhCapCompliances 1 }


cabhCapGroup OBJECT-GROUP
    OBJECTS {
       cabhCapTcpTimeWait,
       cabhCapUdpTimeWait,
       cabhCapIcmpTimeWait,
       cabhCapPrimaryMode,
       cabhCapMappingWanAddrType,
       cabhCapMappingWanAddr,
       cabhCapMappingWanPort,
       cabhCapMappingLanAddrType,
       cabhCapMappingLanAddr,
       cabhCapMappingLanPort,
       cabhCapMappingMethod,
       cabhCapMappingProtocol,
       cabhCapMappingRowStatus,
       cabhCapPassthroughMacAddr,
       cabhCapPassthroughRowStatus
       }
    STATUS    current
    DESCRIPTION
       "Groupe d'objets pour base MIB de portail CAP."
    ::= { cabhCapGroups 1 }


END
```

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	**Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias**
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2005